정보보안 컨설팅

2021.08.09

김수진, 김지원, 이경심, 이지선, 이희진

목 차

□ 위험도 분석 기준

▪ 위험도분석은 개인정보처리시스템에 적용하고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 침해할 위험의 정도를 「위험도 분석 기준」을 이용하여 분석하는 행위입니다. ▪ 「위험도 분석 기준」은 내부망에 고유식별정보를 암호화하지 않고 저장하는 경우 개인정보 처리자가 이행하여야 할 최소한의 보호조치 기준으로 어느 하나의 항목이라도 '아니오'에 해당하는 경우 암호화 대상입니다.

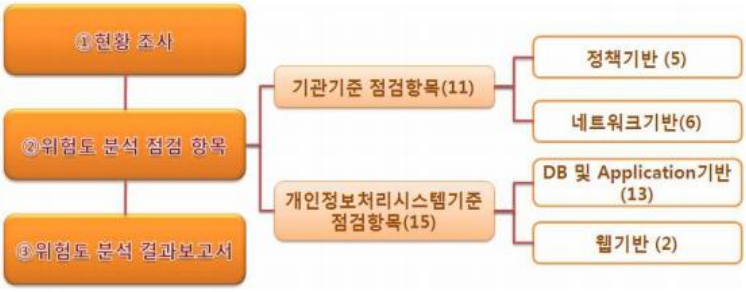
▪ 개인정보처리자는 「위험도 분석 기준」을 허위로 작성해서는 안되며, 「위험도 분석 결과보고서」는 개인정보 보호책임자 또는 해당 부서의 장의 결재를 득한 후 보관 합니다.

▪ 「위험도 분석」은 개인정보파일 단위로 분석하고 결과보고서를 작성하며, 개인정보파일을 위탁한 경우에도 위탁기관이 작성합니다. ※ 결과보고서는 기관의 문서관리 규정에 따라 '대외비' 등으로 관리하시기 바랍니다.

▪ 「위험도 분석」은 최초 분석 이후에도 개인정보처리시스템을 증설하거나, 내.외부망과 연계하거나, 기타 운영환경이 변경된 경우에도 지속적으로 실시하여야 합니다.

□ 위험도 분석 기준 구성

▪ 위험도 분석 기준은 ①현황 조사, ②위험도 분석 점검 항목, ③위험도 분석 결과 보 고서로 구성되어 있습니다.



[그림 1] 위험도 분석 기준 구성

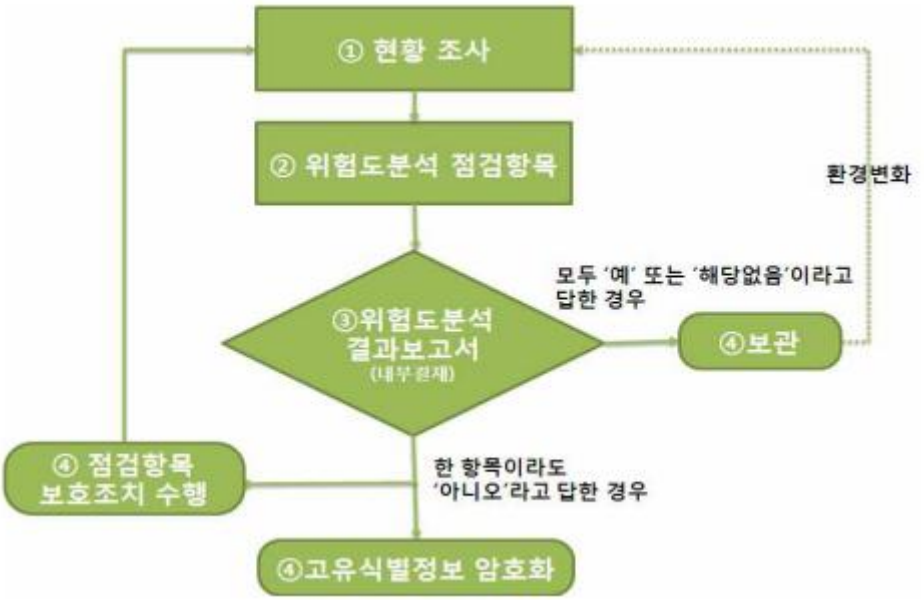
□ 위험도 분석 절차

① 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사

② 개인정보 파일단위별로 위험도 분석 항목별 점검을 수행

③ 위험도 분석 결과보고서를 작성하여 내부결재 후 보관

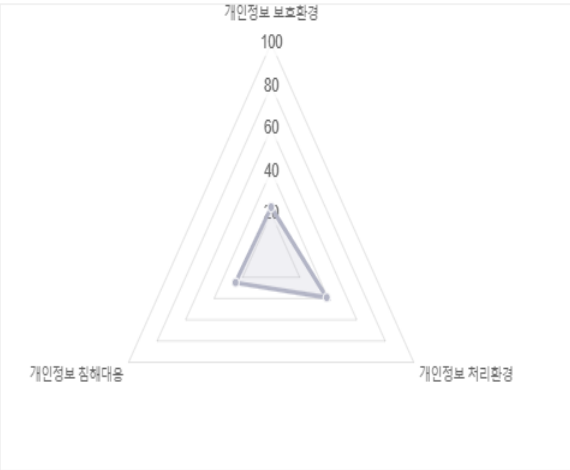
④ 점검 결과에 따라 고유식별정보 암호화 등을 수행

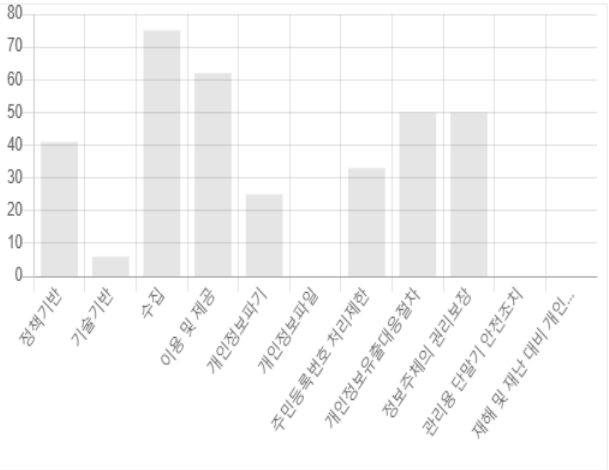


[그림 2] 위험도 분석 절차

진단지표별 진단 수준 점수 : 28.99/100 점

진단 분야별 보호수준





진단분야1	진단분야2	진단지표	보호수준	
개인정보 보호환경	정책기반	1. 개인정보보호 정책 및 자원		42.00%
		2. 개인정보보호 교육		50.00%
		3. 개인정보처리방침		33.00%
	기술기반	5. 개인정보처리시스템 보안운영		25.00%
		6. 개인정보처리시스템의 접근통제		0%
		7. 개인정보 암호화		0%
		8. 개인정보처리시스템 로그 관리		0%
개인정보 처리환경	수집	10. 개인정보 수집 동의		50.00%
		11. 개인정보 수집		100%
	이용 및 제공	12. 이용 및 제공		62.00%
	개인정보파기	13. 개인정보 파기		25.00%
	개인정보파일	14. 개인정보파일 등록 및 운영		0%
	주민등록번호 처리제한	16. 주민등록번호 처리 제한		33.00%
개인정보 침해대응	개인정보유출대응절차	17. 개인정보 유·노출 대응절차		50.00%
	정보주체의 권리보장	18. 정보주체의 권리보장		50.00%
	관리용 단말기 안전조치	19. 관리용 단말기 안전조치		0%
	재해 및 재난 대비 개인정보처리시스템의 안전조치	20. 재해 및 재난 대비 개인정보처리시스템의 안전조치		0%

☐ 현황과 문제점

- J 회사는 현재 홈페이지 회원, 기부회원, 자원봉사자 등 개인 정보를 수집하고 저장하고 있지만 이런 정보들에 대한 목록관리를 하지 않고 있는 상태이고 암호화 하지 않고 인터넷 영역에 저장

☐ 개선 방안

- 관련 업무에 따라 적절한 개인정보 파일 관리를 위해 목록관리파일 샘플 예시를 통해 개인정보파일 목록 작성
- 고유식별정보는 원칙적으로 모든 자리수를 암호화해야 하나, 주민등록번호를 자료 검색키로 사용하는 경우 암호화/복호화에 대한 부하가 발생할 수 있으므로, 속도 등 성능을 고려하여 최소한의 정보만 평문으로 저장하고 이외의 정보를 암호화하는 부분 암호화 조치를 취할 수 있습니다. - 주민등록번호는 생년월일과 성별정보를 포함하고 있는 앞 7 자리를 제외한 뒷자리 6 개 번호 이상 암호화하는 것이 바람직합니다.

  【예시】 700101-1#....&

- 후원회원관리 사이트의 경우 비밀번호와 고유식별정보가 암호화되어 전송 및 저장되는지 프로그램 제공업체에 확인
- 고객정보가 포함된 서류는 잠금장치가 있는 곳에 보관, 담당자를 지정하여 관리

〈개인정보파일 목록 작성 예시〉

□□□□□□□ □□□□ □ □□ □□		JAKOREA	JAKOREA	JAKOREA
□□□		□□□□□	□□□□□	□□□□□
□□□□□		□□□	□□□	□□□
□□□□		□□□□	□□□□	□□□□
□□□□□□□□□□□ □□		JAKOREA □□□□	□□□□□□□	□□□□□□□
□□□□□□□ □□		JAKOREA □□□□ □□□□	□□□□□□□	□□□□ □□
□□□□□□□ □□ □□		□□□□ □□□ □ 15□ □ 1□ □ 1□ (□□□□□ □□)	□□□□ □□□ □ 15□ □ 1□ □ 1□ (□□□□□ □□)	□□□□ □□□ □ 15□ □ 1□ □ 1□ (□□□□□ □□) □□□□ □ 112□ □ 2□ 1□
□□□□□□□ □□ □□		□□ □□ (□□.□□.□□ □)□□.□□.□□ □ □□□ □□□ □□	□□□□□ □□□□□□	□□□□ □□ □ □□□□□□ □□
□□□□□□ □ □□□□ □ □□□□ □□	□□□□ (□ □□□□ □ □□□ □□ □)	□□□□ :□□.□□□, E-Mail, □□□.□□□□.□□ □□□□ :	□□□□ :□□.□□□, E-Mail, □□□.□□□□.□□ □□□□ :□□□□ (□□),□□.□□/□□.□□/□□□. □□□□.□□□□□□	□□□□ :□□.□□□, E-Mail, □□□.□□□□.□□.□□ □.□□□□ □ □□□□.□□□ □□□□ (□□□□ :□□□. □□□□.□□□□.□□□ □□□□ (□□□□□□□□),□□□ /□□□□ :□□□.□□□□.□□□□),□□□□.□□□□ □□□□ :□□□.□□□□□□ (□□□□□□ □□ □□ □), □□□□□)
	□□□□□ (14□ □□ □ □□ □)	□□□□ :□□.□□□ □□□□ :	□□□□ :□□.□□□ □□□□ :	□□□□ :□□.□□ □□□□ :
□□□□□ □□□□		□□□ □□ (□□□□ □□□□.□□□□ □)	□□□□ □□ (□□□ □□□□ □□ □□ □□) □□□ □□ (□□□□ □□□□.□□□□ □)	□□□□ □□ (□□□ □□□□ □□ □□ □□) □□□ □□ (□□□□ □□□□.□□□□ □)
□□□□□ □□□□		□□□□□	□□□□□	(□□ □□ □) (10□)
□□□□□ □□□ □□ □□□□□ □□□□ □□	□□□□□	□□ □□□□□□ □□□□ □□□□ □□.	□□ □□□□□ □□□□□ □□□□ □□□ □ □□.	□□□ (□□□□□□ □□ □□□□ □□),□□□□□
	□□		□□	□□□ :□□□□ □ 112□ □ 2 □□□□□ :□□□□□ □□
	□□□□□ □□		□□	□□.□□□□□□.□□□□.□□□□ /□□□.□□□□. □□□□.□□□.□□□□ (□□□□□□□□),□□□
□□□□□□□ □□□□ □ □ □□□□□ □□□□ □		□ 31,450 □	206□	□ 100□
□□ □□□□ □□□□ □□ □□ □□□ □ □□□ □□	□□	□□ □□□□□□ □□□□ □□□□ □□.	□□ □□□□□ □□□□□ □□□□ □□□ □ □□.	□□ □□□□□ □□□□□ □□□□ □□□ □ □□.
	□□□□□□	□□□□ □□□□	□□	□□□□ □□□□ □□

구분	점검항목
정책기반	1. 개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?
	2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립. 운영하고 있습니까?
	3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?
	4. DB 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W 만 사용하도록 하는 정책을 수립. 운영하고 있습니까?
	5. DB 서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연 2 회 이상 실시하고 있습니까?

□ 현황과 문제점

- 개인정보취급방침에 담당자가 명시되어 있지만 정책, 책임, 권한 및 역할 정의가 되어 있지 않음
- 내부관리계획, 개인정보보호 추진계획, 개인정보보호 관련 각종 내부지침 부재
- 외주 보안관리 현황 문서 부재
- 불법 또는 비인가된 S/W 사용 관리 부재

□ 개선방안

- 개인정보보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으므로 당해 조직의 구성원 전체에 통용되는 내부 규정 마련
- 개인정보 침해사고에 대비하여 침해사고시 대응 절차, 담당자, 피해복구조치 등 침해 대응 계획
- '개인정보취급자'는 기업. 단체. 공공기관의 임직원, 계약직원, 아르바이트 직원 등의 시간제 근로자뿐만 아니라 외부기관에서 또는 외부기관으로 파견된 근로자 등도 해당.
- 최근의 개인정보 유출사례를 보면 개인정보취급자에 대한 관리 소홀, 특히 외주 인력에 대한 보안관리 소홀이 그 원인이 되는 경우가 많으므로 보안서약서 집행, 비밀번호 노출 예방 등 외주 인력의 보안관리 조치 수행 - 외주 보안관리 현황 작성
- **윈도우에서 제공하는 PC 방화벽 설정**

  ※ 자세한 설정 방법은 http://www.privacy.go.kr → 배움터 → 사이버교육 → "업무용 PC 에서의 개인정보 보호조치 설정 방법" 3 차시 '접근통제시스템 설치 및 운영' 동영상을 참조
- 개인정보보호교육 - 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으며, 조직의 여건 및 환경을 고려하여 집체 교육, 온라인 교육 등 다양한 방법 활용하고 교육 목적, 대상, 내용, 일정 및 방법 등을 포함하는 'OO 년 개인정보보호 교육계획', 교육결과보고

*** 개인정보 보호위원회의 '개인정보보호 포털'(www.privacy.go.kr)에서 제공하는 교육 프로그램 및 교육교재 등 활용 가능**

- 개인 유지보수나 AS 를 위해 PC 를 업체로 이동시키거나 유지보수업체에서 PC 에 원격으로 접속하는 경우 유지보수업체가 개인정보에 함부로 접근하지 못하도록 업무 위탁에 관한 사항을 문서화하여 개인정보유출사고 발생시 책임소재 소명 (유지보수 계약서에 포함 가능)

구분	점검항목
네트워크 기반	6. 상시적으로 비인가 IP 주소의 접근을 통제하고 있습니까?
	7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?
	8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?
	9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?
	10. 주기적으로 네트워크 접속에 대한 로그를 관리하고, 분석하고 있습니까?

□ 현황과 문제점

- 네트워크 기반 보호조치 부재

□ 개선방안

- 악성 프로그램 등을 통해 개인정보가 위.변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치.운영하고 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1 회 이상 업데이트를 실시하여 최신의 상태로 유지
- 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
- 발견된 악성프로그램 등에 대해 삭제 등 대응조치

*** 한국인터넷진흥원의 "보호나라" 참조**

구분	점검항목
DB 및 Application 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?
	13. DB 서버내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?
	16. DB 서버에 접속하는 관리자 PC 가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동 발생시 지체없이 DB 접근권한을 변경하고 있습니까?
	19. DB 접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3 개월마다 변경하고 있습니까
	20. DB 접속자 및 개인정보취급자의 비밀번호 입력시 5 회 이상 연속 입력오류가 발생한 경우 계정잠금 등 접근을 제한하고 있습니까
	21. DB 및 DB 접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까
	22. DB 및 DB 접속 어플리케이션 서버에서 보조기억 매체(USB 등) 사용시 관리자 승인 후 사용하고 있습니까?
	23. DB 서버 및 DB 접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까
	24. HDD 등 DB 저장매체의 불용처리시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
웹(Web) 기반	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년 1 회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위. 변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?

□ 현황과 문제점

- DB 및 Application 기반 보호조치 부재
- 웹(Web)기반 보호조치 부재

□ 개선방안

- 개인정보취급자의 역할에 따라 조회, 등록, 수정, 삭제 등의 권한을 업무수행 목적에 따라 최소한의 범위로 차등화하여 부여

  【예시】 회계부서는 영업부서 화면에 접근하지 못하도록 권한 부여

- 개인정보취급자의 전보, 이직, 퇴사 등으로 인해 계정의 변경. 삭제가 필요한 경우 즉시 계정 삭제 및 패스워드 변경 등 DB 접근권한 변경

- 비밀번호를 장기간 사용할 경우, 그만큼 비밀번호 해킹의 가능성도 높아지므로 비밀번호의 유효기간을 설정하여 최소 3 개월마다 변경

- 개인정보처리시스템의 서버에 비인가자의 물리적 접근 관리

  【예시】수기문서 대장 기록방법 : '출입자', '출입일시', '출입목적' 등을 출입관리 대상에 기록

- 저장매체의 폐기, 양여, 교체 등 불용처리로 저장매체에 저장된 개인정보는 모두 파기해서 외부에 노출되지 않도록 해야 하며, 복구될 수 없도록 완전하게 삭제, 하드디스크를 포맷한 후 중고 PC 로 매매하는 경우가 종종 있으나, 파일 삭제 또는 하드디스크 포맷만으로는 데이터 영역이 완전하게 삭제되지 않아 복구될 수 있고 중고 PC 에 개인정보가 남아 있을 경우 개인정보 오.남용의 위험성이 있으므로 이를 방지하기 위한 조치가 필요

  【예시】국가정보원이 저장매체 불용처리 지침

저장매체	삭제 방법
플로피 디스크	완전파괴(소각, 파쇄, 용해)
광디스크(CD, DVD)	완전파괴(소각, 파쇄, 용해)
자기 테이프	완전파괴(소각, 파쇄, 용해) 또는 전용 소자(消磁)장비이용 삭제
반도체 메모리 (EEPROM 등)	완전파괴(소각, 파쇄, 용해) 또는 완전포맷 3회 수행
하드디스크	완전파괴(소각, 파쇄, 용해) 또는 전용 소자(消磁)장비이용 삭제 또는 완전포맷 3회 수행

- 개인정보보호 포털 개인정보보호 기술지원 활용 : 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치에 어려움을 겪는 중소기업·소상공인을 대상으로 개인정보보호 기술상담 및 온라인 컨설팅, 현장방문 컨설팅 등을 지원
  (https://www.privacy.go.kr/a3sc/per/tec/req/tecSupportReq.do)

□ 현황과 문제점

- 중요정보와 주요직무 별 부서가 존재하지 않음
- 중요정보 및 주요직무에 대한 정의 확립이 필요함

□ 개선방안

- 중요정보(개인정보, 인사정보, 영업비밀, 재무정보)와 정보시스템, 정보보호시스템, 정보보호 관리업무 수행, 보안시스템 운영자를 주요직무자로 지정해야합니다.

□ 현황과 문제점

- IT 부서가 존재하지 않으며 개인정보보호 담당은 경영기획팀이 총괄함

□ 개선방안

- IT 부서가 존재하지 않고 경영기획팀이 개인정보 관련한 업무를 총괄하고 있으므로 직무 미분리시 통제 현황에 대한 증적이 필요합니다.

□ 현황과 문제점

- 계약서상 비밀유지서약 문장이 포함되어 있으며 임시직원과 외주용역에 정보보호에 대한 책임을 명시한 정보보호서약을 별도로 받고 있지 않음
- 퇴사 시에는 내부 정보자산 유출금지에 대한 문장이 포함되어 있음
- 법적 분쟁 발생 시 증거자료로 사용하기 위해 비밀유지 서약서를 인사회계팀이 별도로 보관중에 있음

□ 개선방안

- 임시직원과 외주용역에게 정보보호에 대한 책임을 명시한 비밀유지서약을 별도로 받는 것을 권장합니다.
- 고용 조건의 변경 등 중요 변경사항 발생 시 서약서 재작성 등의 조치 수행이 필요합니다.
- 인사회계팀이 비밀유지 서약서를 안전하게 보관하기 위해 안전한 보관규칙을 따라야 합니다.

예)

법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있도록 잠금 장치가 있는 캐비닛 또는 출입통제가 적용된 문서고 등에 안전하게 보관/관리 해야 합니다.

-

□ 현황과 문제점

- 개인정보보호에 대한 온라인 교육을 재직자/신입 구분없이 4 분기에 매년 진행중에 있음
- 휴직자를 제외하고 모두 교육이수 진행 중이며 휴직자의 경우 복직하고 난 이후 재직자/신입과 함께 교육 진행함
- 7 일 중 하루를 선택하여 교육을 진행중이기에 불참하는 경우가 없으며 해당 교육에 대한 교육결과 보고서와 교육 참석자 목록을 문서화 하고 있음

□ 개선방안

- 코로나 시대에 맞춘 피시점검 유의사항, 임직원 PC 자가진단, 재택근무 유의사항, 업무 PC/개인 PC 별 주의사항을 추가적으로 교육하는 것이 바람직합니다.
- 상황에 맞춘 주기적인 보안공지와 보안 캠페인을 통해 임직원들로 하여금 개인정보보호에 관한 관심을 상기시키는 것이 중요합니다.

가이드라인)

- 재택근무, 원격협업, 스마트워크 등과 같은 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호대책을 수립·이행하여야 한다.
  - 스마트워크 업무형태 정의 : 재택근무, 스마트워크 센터, 원격협업, 모바일오피스 환경
  - 스마트워크 업무형태에 따른 업무 허가 범위 설정 : 내부 시스템 및 서비스 원격접근 허용 범위
  - 스마트워크 업무 승인절차 : 스마트워크를 위한 원격접근 권한 신청, 승인, 회수 등
  - 원격접근에 필요한 기술적 보호대책 : 전송구간 암호화(VPN 등), 강화된 사용자 인증(OTP 등)
  - 접속 단말(PC, 모바일기기 등) 보안 : 백신 설치, 보안패치 적용, 단말 인증, 분실/도난 시 대책(신고 절차, 단말잠금, 중요정보 삭제 등), 중요정보 저장 금지(필요 시 암호화 조치) 등
  - 스마트워크 업무환경 정보보호지침 수립 및 교육 등

-

□ 현황과 문제점

- 상벌규정과 징계절차는 별도로 존재하지 않으며, 위반사항이 발견된 경우 내부상벌 위원회 결정사항에 따라 조치함
- 개인정보 지침 위반자에 대한 징계내역은 아직까지 없기에 문서화되어있지 않음

□ 개선방안

- 임직원 및 관련 외부자가 법령과 규제 및 내부정책에 따른 정보보호 및 개인정보보호 책임과 의무를 위반한 경우에 대한 처벌규정을 수립해야 합니다.

㉠관련 법규 및 내부 규정 미준수, 책임 미이행, 중요정보 및 개인정보의 훼손, 유/노출, 오/남용 등이 발견된 경우 조사, 소명, 징계 등의 조치 기준 및 절차 수립

㉠정보보호 및 개인정보보호 책임과 의무를 충실히 이행한 경우에 대한 보상 방안도 고려

□ 현황과 문제점

- 외부자가 계약 만료 시 중요정보를 파기 했다는 파기 확약서를 받고 있음

□ 개선방안

- 파기 확약서 작성 시 보유기간 경과나 처리목적 달성 시 지체없이 개인정보를 파기한다는 사실을 명시해야 합니다.
- 이 외, 개인정보를 보존해야 하는 상황에는 예외적인 기재를 해야 합니다.
- 파기 절차 및 방법을 분명하고 구체적으로 명시하여야 합니다.

-

□ 현황과 문제점

- 어플리케이션을 구매하여 이용하고 있으며, 경영기획팀 담당자만 접근가능함
- 인사정보시스템 사용자에 대한 보안서약서가 개별적으로 존재하지 않으며 보안서약서에 정보보호에 대한 내용이 총체적으로 포함됨
- 인사정보시스템의 보안성 점검을 수행하지 않음

□ 개선방안

- 인사정보시스템 보안성 점검 수행이 필요합니다.

보안성 검토를 실시해야 하는 경우(자료: 이글루시큐리티)

1. 물리적 보안구역의 신설 및 변경 시
2. 전산실을 신규로 설치하는 경우
3. 내부 정보통신망을 인터넷 등 외부 공개 네트워크와 연결하는 경우
4. 무선랜 등 무선망을 사용해 업무를 처리하거나 원격근무 지원 등을 위해 시스템을 도입하는 경우
5. 보안장비 및 암호화 프로그램 등 정보보호시스템을 도입하는 경우
6. 정보통신 운영환경 변화로 인하여 보안성 검토가 필요하다고 인정되는 경우
7. 정보시스템 업무를 외부에 용역 의뢰하는 경우(핵심업무의 개발 및 운영 전체를 용역하는 경우)
8. 외부기관에 보안감리 또는 보안컨설팅을 의뢰하거나 정보처리·보안 관제 등의 업무를 위탁하는 경우
9. 정보시스템의 운영 환경 및 정보자산에 중대한 변화가 발생한 경우
10. 중요한 정보자산 도입 설치 및 신규 사업을 추진하는 경우
11. 물리 보안관리부서의 요청이 있는 경우
12. 정보시스템 운영부서의 요청이 있는 경우
13. 기타 보호관리자가 필요하다고 인정하는 경우

참고) 보안성 검토 체계 수립과정

https://www.comworld.co.kr/news/articleView.html?idxno=49506

J 회사 정보보안 현황 점검 항목[이경심]

□ 정책, 조직, 정보자산 관리

구 분	점 검 항 목	예	아니오	비 고
정책, 조직의 관리	1. 정보보호 및 개인정보 관리체계가 효과적으로 운영되기 위한 정책 지침 및 그에 따른 절차가 있는가?	√		
	2. 정보보호 지침을 수립, 운영하기 위한 관련 업무를 담당하는 사내 조직이 있는가?	√		담당하는 조직(경영기획 팀)이 있지만 현재 해당 업무를 진행하고 있지 않음
	3. 수립된 정책 및 시행문서를 정기적으로 검토 및 필요, 변경 여부에 따라 제·개정하고 관련 정책 및 시행문서의 제·개정 시 이해 관계자의 검토를 받고 있는가?		√	재 개정 내역을 관리하지 않음
	4. 정보보호 관리조직은 관련법령 개정사항에 대하여 모니터링을 하고 있는가?	√		
	5. 각 사업 부서별 정보보안 정책이나 지침을 다르게 정하고 실행하는가?		√	사업 홈페이지 등 개설 시 업데이트된 개인정보보호 정책을 적용 및 업무에 대한 부분은 지침이 다르진 않습니다
정보자산관리	1. 정보자산 관리를 위한 정보자산 등급에 따른 취급절차(생성, 도입, 저장, 이용, 파기) 및 보호대책을 마련하고 있는가?		√	
	2. 정보자산의 분류기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하는가?		√	
	2-1. 식별된(목록화된) 정보자산에 대한 관리자 및 책임자는 지정되어 있는가?		√	
	3. 정보자산 목록은 정기적으로 현황을 조사(반기 또는 연1회 이상)하여 최신으로 유지하는가?		√	

정보자산관리 및 주요 직무자 지정 관리	1. 식별된 정보자산에 대해 법적 요구사항 및 업무에 미치는 영향 등을 고려하여 중요도를 결정하고 보안등급을 부여하고 있는가?		√	
	1-1. 업무관련 문서의 중요도 및 등급(기밀, 일반공개 등)을 나누는 내부 기준이 있는가?		√	가이드나 보안등급은 없지만, 일반적으로 주민등록번호, 급여 등의 회계자료는 회계담당자와 총장님만 접근 가능
	1-2. 중요도에 따라 보호 대책의 수준의 차이가 있으므로 중요도 등급에 따른 보호 대책을 마련하고 있는가?		√	
	2. 정보보호 및 개인정보 관리체계에 따른 현황 점검을 실시하고 있는가? (내부감사, ISMS 등 정보보호 활동에 대한 점검 활동)		√	
	2-1. 관리체계 점검계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 경영진에게 보고하는가?		√	
점검항목 결함	• 정보보호 지침을 수립, 운영하기 위한 관련 업무를 담당하는 조직(경영기획팀)이 있지만, 현재 수립된 정책 및 시행문서를 정기적으로 검토를 하고 있지 않음 • 정보보호 관리체계 정책의 변경 여부를 제·개정하여 관리하거나, 문서화 하지 않고, 이해 관계자의 검토를 받고 있지 않음 • 정보자산별 담당자 및 책임자를 식별하지 않았고, 자산목록 현행화가 미흡 • 정보자산에 대한 중요도 평가를 실시하여 보안등급을 부여 후 등급에 따른 취급절차 정의, 정보자산 목록화할 필요 있음			

□ 인증 및 권한관리

구분	점검항목	예	아니오	비고
사용자 계정관리	1. 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자가 조직의 인프라(서버, 네트워크, 데이터베이스 등)와 응용프로그램(업무활용 프로그램, 인사시스템, 그룹웨어, 회계시스템 등)에 접근 시 계정 및 접근권한 발급 절차를 수립하고 이행하는가?		√	별도의 승인 절차 없지만, 입,퇴사자에 따라 관리자가 접근권한을 관리
	2. 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성·등록·변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가?		√	
	2-1. 사내 계정관리 보호조치 적용은 이루어지고 있는가? (예: 계정 만료일 등록, 일정기간 미사용 시 계정 잠금, 퇴사자 적용 등)	√		퇴사 시 계정 비밀번호 변경 / 자료 백업 등 필요 없을 시 비활성화 조치
	2-2. 사용자 계정관리 절차의 계정발급 및 권한부여 현황 목록을 관리하고 점검하는가?		√	
	3. 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시키고 있는가? 어떠한 과정을 통해 해당 계정에 대한 보안책임 인식을 교육하는가?		√	연 1회 공통적으로 개인정보 보호 관련 교육만 진행함
	4. 계정관리 시스템과 데이터베이스의 접근관리 솔루션이 있는가?	√		홈페이지, 드라이브 등은 외부업체, 업무틀은 office365를 사용
	5. JA Korea의 현 업무 환경은 대면·비대면을 병행, 비대면 업무(원격근무) 시 정보보안 강화를 위한 계정관리 가이드가 있는가?		√	
	6. JA Korea 임직원의 비대면 업무(원격 업무) 시, 전용 접속환경	√		VPN(가상사설망) 이용 MS One-Drive 이용

사용자 식별	1. 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자(예: 아이디)를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가?		√	모든 직원이 이름 이니셜로 아이디를 사용 ex) hjpark
	2. 불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 중 외부에서 내부 시스템에 접근(외부업체 또는 기관과의 공유계정이 사용) 하는 경우가 있는가?	√		MS 원드라이브에 파일을 생성, 해당 파일 링크만 공유하여 해당 파일의 데이터가 취합되도록 함
	2-1. 내부인이 아닌 외부인에게 계정발급 시 어떠한 방식으로 계정발급이 이루어지는가?		√	외부인의 계정발급이 이루어지지 않으나, 만약 필요시 접근권한을 제한하여 발급할 수 있음
	2-2. 공유계정을 사용하는 경우, 실사용자가 누구인지 확인할 수 있는 수단이 있는가?	√		엑세스 현황 확인 가능 (MS Office365)
사용자 인증	1. 정보시스템 및 개인정보처리시스템에 대한 접근 시, 안전한 사용자 인증 절차에 의해 통제하고 있는가?	√		
	1-1. 계정 도용 및 불법적인 인증시도 시 어떠한 통제방안이 있는가?	√		로그인 실패 횟수 제한 불법 로그인 시도 경고
	2. 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는, 법적 요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용하고 있는가?			
비밀번호 관리	2. 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성 규칙을 수립·이행하고 있는가?		√	규칙은 없지만 비밀번호에 특수문자, 대문자 등 활용하는 편
	2-1. 비밀번호 작성규칙을 불가피한 경우를 제외하고 시스템적으로 강제화 하는가?	√		

사용자 식별	1. 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자(예: 아이디)를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가?		√	모든 직원이 이름 이니셜로 아이디를 사용 ex) hjpark
	2. 불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 중 외부에서 내부 시스템에 접근(외부업체 또는 기관과의 공유계정이 사용) 하는 경우가 있는가?	√		MS 원드라이브에 파일을 생성, 해당 파일 링크만 공유하여 해당 파일의 데이터가 취합되도록 함
	2-1. 내부인이 아닌 외부인에게 계정발급 시 어떠한 방식으로 계정발급이 이루어지는가?		√	외부인의 계정발급이 이루어지지 않으나, 만약 필요시 접근권한을 제한하여 발급할 수 있음
	2-2. 공유계정을 사용하는 경우, 실사용자가 누구인지 확인할 수 있는 수단이 있는가?	√		엑세스 현황 확인 가능 (MS Office365)
사용자 인증	1. 정보시스템 및 개인정보처리시스템에 대한 접근 시, 안전한 사용자 인증 절차에 의해 통제하고 있는가?	√		
	1-1. 계정 도용 및 불법적인 인증시도 시 어떠한 통제방안이 있는가?	√		로그인 실패 횟수 제한 불법 로그인 시도 경고
	2. 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는, 법적 요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용하고 있는가?	√		
비밀번호 관리	2. 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성 규칙을 수립·이행하고 있는가?		√	규칙은 없지만 비밀번호에 특수문자, 대문자 등 활용하는 편
	2-1. 비밀번호 작성규칙을 불가피한 경우를 제외하고 시스템적으로 강제화 하는가?	√		

	2-2. 비밀번호 작성규칙은 조합 규칙 적용, 변경주기 설정, 추측하기 쉬운 비밀번호 설정 제한, 동일한 비밀번호 재사용 제한이 있는데 작성규칙을 이행하고 있는가? (비밀번호의 자리수, 복잡도 설정(대문자, 숫자, 특수문자 등), 비밀번호 유효기간에 대해서도 어떤 정책을 마련하고 있는가?		√	3개월마다 강제로 변경하는 경우도 있고, 1년 내 변경하지 않는 경우도 있음
	3. 비대면 근무(원격근무) 환경 시, 근무자의 비밀번호 보안 가이드를 공지하고 있는가?		√	
특수계정 및 권한관리	1. 관리자 등 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립, 이행하고 있는가?		√	관리자 등 특수 권한은 경영기획팀 내 담당자만 부여 받음 (신청, 승인 절차는 없음)
	2. 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하는가?	√		특수 목적을 위한 계정은 별도로 관리함
	3. 특수권한자 현황을 정기적으로 검토하여 목록 현행화를 이행하고 있는가?		√	
접근권한 검토	1. 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남기고 있는가?		√	
	2. 접근권한 검토 결과 권한의 과다 부여, 절차 미준수, 권한 오.남용 등 의심스러운 상황이 발견된 경우 그에 따른 조치절차를 수립.이행하고 있는가?	√		해당 사례가 발생한 적이 없어 구체적인 조치절차를 수립하고 이행한 사례는 없으며 직무변경, 퇴직 등 발생 시 접근 권한을 제한하고 있음
	3. 접근권한 검토 후 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지하는가?	√		

점검항목 결함	• 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자가 조직의 인프라와 응용프로그램에 접근 시 계정 및 접근권한 발급 절차의 명시 및 별도의 승인 절차 필요 • 정보시스템을 사용하기 위한 계정을 신청하는 경우에는 사용자 계정 신청서를 작성해 전자결재시스템 등을 이용해 해당 정보시스템을 관리하고 있는 부서 책임자의 승인을 받아야 함 • 책임자의 승인이 확인된 경우에 한해 사용자 계정 생성 및 권한 부여 필요, 관련 내용 기록 포함해야 함 • 중요정보를 취급하는 직무별 또는 역할별로 분류 체계를 작성하여 접근 권한을 정의하고, 정보시스템에 대한 접근권한은 업무 수행에 필요한 최소한으로 할당하고 최소인원에 대해 할당해야 함 • 사용자에게 계정 및 접근권한을 부여하는 경우 정보보호정책, 서약서 등을 통해 계정에 대한 책임은 사용자에게 있음을 명기하고 이메일, 공지, 교육 등을 통해 지속적으로 인식을 제공해야 함 • 중요하다고 생각하는 데이터를 보유한 정보시스템에 로그인하는 경우 2Factor 인증 등 강화된 인증 방식 사용할 것 • 내부 관련 지침 등에 비밀번호에 대한 변경 절차를 명시하고 있고 이에 따라 정보시스템에서 임시, 초기 비밀번호 변경, 주기적인 비밀번호 변경을 수행해야 함 • 이용자가 이용하는 웹 서비스에 대한 안전한 비밀번호 작성 규칙의 수립 및 강제화 적용 해야 함 • 정보시스템 유지보수 등을 위해 외부자에게 제공된 계정이 절차에 따라 관리되어야 함 • 모든 정보시스템(서버, 네트워크, 정보보호솔루션, 응용시스템 등)에 생성된 사용자 계정 및 접근권한에 대해 정기적으로 검토하는 기준과 절차를 마련해야 함 • JA Korea의 현 업무 환경은 대면·비대면을 병행, 비대면 업무(원격근무) 시 정보보안 강화를 위한 계정관리 가이드 필요

JA Korea 정책,조직, 자산 관리
인증 및 권한관리 [이경심]

[정책, 조직, 자산 관리]

기준	J 회사의 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되기 위한 정책지침 및 그에 따른 절차를 수립하고, 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토해 필요한 경우 제·개정하고 그 내역을 이력 관리해야 합니다.
확인 사항	1. 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책을 수립해야 합니다. - 정보보호 정책에는 경영진의 정보보호에 대한 의지, 정보보호 목적, 범위, 책임, 조직이 수행하는 관리적, 기술적, 물리적, 정보보호 활동의 근거를 포함해야 합니다. J 회사에서 제공하는 서비스에서 준수해야 하는 정보보호 관련 법적 요구사항을 포함해 정보보호지침, 절차, 매뉴얼 등의 형식으로 수립해야 합니다. 클라우드 서비스 이용함에 있어 클라우드 서비스 운영 지침, 절차, 매뉴얼과 같은 문서를 클라우드 서비스 제공 모델 및 유형에 따른 보안 요구 사항을 반영해 수립해야 합니다. 2. 정보보호 및 개인정보보호 관련 정책 및 시행문서에 대한 정기적인 타당성 검토 절차를 수립, 이행하고 이해관계자의 검토 및 개정이력에 대한 관리를 수행해야 합니다. - 정보보호정책이 상위조직 및 관련 기관 정보보호정책과의 연계성이 있는지 타당성을 검토해야 하며, 정보보호정책·지침 제·개정, 폐기 시 이력(일자, 내용, 작성자, 승인자 등)을 확인할 수 있는 관리절차를 수립하고 이행해야 합니다. 또한, 조직의 대내외 환경의 중대한 변화 발생 시 정보보호 및 개인정보보호 관련 정책 및 시행문서에 미치는 영향을 검토하고 필요 시 제·개정해야 합니다. - 정보보호정책· 지침 제·개정을 검토한 경우 제·개정 시 실제 정책을 적용 받는 부서와 타당성을 검토해 반영하고 최고경영자 또는 정보보호 최고책임자의 승인을 받아 지침 제·개정을 확정하고 임직원에 공표해야 합니다. 지침 제·개정과 관련된 경영진 승인 및 지침 제·개정 이력은 증적이 남을 수 있도록 관리해야 합니다.
관련 법규	정보통신망법 제 28 조(개인정보의 보호조치) 개인정보 보호법 제 29 조(안전조치의무) 개인정보의 안전성 확보조치 기준 제 4 조(내부관리계획의 수립, 시행) 개인정보의 기술적, 관리적 보호조치 기준 제 3 조(내부관리계획의 수립, 시행)

□ 현황과 문제점

- 정보보호 및 개인정보보호 관리체계가 효과적으로 운영을 위한 정책 및 시행문서의 부재 및 내용 미흡
- 정보보호 및 개인정보보호 관련 법령, 고시 등에 변경사항이 발생 시, 시행문서에 미치는 영향을 검토 후, 변경 사항을 반영한 제·개정 내역의 관리 미흡
- 정보보호 및 개인정보보호 관련 시행문서의 정기적인 검토 및 제·개정 시 이해 관계자의 검토 필요

□ 개선방안

- **정책은 정보보호 활동을 규정한 상위 정보보호정책과 상위 정책 시행을 위한 문서(지침, 절차, 매뉴얼 등)로 구분해 제정합니다. 문서의 제 · 개정 시에는 이해 관계자의 검토(협의 및 조정)를 통해 정책, 지침, 절차에서 정하고 있는 정보보호 활동의 주기, 수준, 방법 등을 정의하고 일관성 있게 유지해야 합니다. 클라우드 서비스의 운영 지침, 절차, 매뉴얼과 같은 문서도 클라우드 서비스 제공모델과 유형에 따른 보안 요구 사항을 반영해 수립해야 합니다.**

- **정보보호정책 제 · 개정 시에는 정보보호 활동에 대한 경영진의 참여와 지원을 보장하기 위해정보보호정책은 최고 경영자의 승인을 받아야 하며 지침 · 절차 등 정책시행 문서는 최고경영자의 승인을 받거나 최고경영자의 위임을 받은 정보보호 책임자의 승인을 받아야 합니다. 또한, 정보보호 및 개인정보보호정책은 임직원들이 준수해야 하는 내용을 포함하고 있기 때문에 조직에서 운영하고 있는 그룹웨어, 이메일, 사내 메신저 등을 통해 즉시 공지하고 최신본을 임직원이 쉽게 접근할 수 형태로 제공해야 합니다.**

- **정보보호 및 개인정보보호 관련 정책 및 시행문서에 대하여 정기적인 타당성 검토 절차를 수립 · 이행하고, 필요 시 관련 정책 및 시행문서를 제 · 개정하여야 합니다.**

  〉정기 타당성 검토 절차 수립 시 포함되어야 할 사항

  - 검토 주기 및 시기: 연 1 회 이상 검토 필요
  - 관련 조직 별 역할 및 책임
  - 담당 부서 및 담당자
  - 검토 방법
  - 후속조치 절차: 정책 및 시행문서 제·개정이 필요한 경우 관련 절차, 내부 협의 및 보고 절차 등

- **정보보호 관리자는 대내외적 업무 환경 및 법률의 변화가 발생하였을 경우 정보보호정책을 검토하고 반영해야 합니다.**

  정보보호 및 개인정보보호 관련 법규 제·개정

  조직 환경의 변화(신규사업, 조직개편 등)

  새로운 위협 또는 취약점 발견

정보시스템 및 정보보호 환경의 중대한 변화(신규 보안시스템 또는 IT 시스템 도입 등)

내부감사 수행 결과

- **정보보호 관리자는 정보보호정책 변경이 필요할 경우다음 절차에 따라 변경합니다.**

  관련 전문가 및 해당 실무자의 검토

  정보보호위원회 검토 및 대표이사 승인

  개정된 정책 게시, 공고 및 교육

  개정된 정책의 적용 및 준수

- **정책의 점검을 통해 제·개정이 발생하는 경우에는 각 정책·지침에 다음과 같이 검토일, 제·개정 내용, 담당자, 승인자 등이 포함된 이력을 남겨 어떤 부분이 변경됐는지 확인할 수 있도록 해야 합니다.**

  〉정보보호정책·지침 제·개정이력(예시)

날짜	제·개정 내용	담당자	승인자
2021.08.07	지침 신규 제정	정보보호팀 정보호	CISO 최보안

기준	J 회사내 담당 조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 구성원 간 상호 의사를 소통할 수 있는 체계를 수립하고 운영해야 합니다.
확인 사항	1. 정보보호 및 개인정보 관련 책임자와 담당자의 역할 및 책임을 명확히 정의하고 활동을 평가할 수 있는 체계를 수립해야 합니다. - 정보보호 관리자, 정보보호 담당자 등 정보보호실무자는 정보보호 최고책임자의 관리 업무를 실무적으로 이행할 수 있도록 직무기술서 등을 통해 책임과 역할을 구체적으로 정의해야 한다. 정보보호 활동이 적절히 이뤄지고 있는지 지표로 측정할 수 있는 목표와 성과지표(Objectives and Key Results), 조직내 핵심성과지표(Key Performance Indicator) 등과 정량적인 측정 체계를 구성해야 합니다. 2. 개인정보 보호책임자는 조직의 개인정보보호 관련 법령 준수 여부를 지속적으로 확인하여 위반 사실을 알게 된 경우 지체 없이 개선조치하고, 필요시 그 사실을 최고경영자 또는 경영진에 보고하여야 합니다(정보통신망법 제 27 조 제 4 항) 3. 정보보호 최고책임자와 최고경영자 간의 소통, 정보보호부서와 기획부서 등 다양한 부서들이 소통할 수 있는 커뮤니케이션 체계를 마련해야 합니다.
관련 법규	개인정보 보호법 제 29 조(안전조치의무), 제 31 조(개인정보 보호 책임자의 지정) 정보통신망법 제 27 조(개인정보 보호책임자의 지정), 제 28 조(개인정보의 보호조치), 제 45 조의 3(정보보호 최고책임자 지정 등) 개인정보의 안전성 확보조치 기준 제 4 조(내부관리계획의 수립·시행) 개인정보의 기술적·관리적 보호조치 기준 제 3 조(내부관리계획의 수립·시행)

□ 현황과 문제점

- 기업 조직에서 개별 프로세스 및 조직의 구성원들이 수행해야할 **'역할'**과 그 역할의 수행에 따른 **'책임'** 관계를 보여주는 R&R (Role and Responsibilities)을 확인할 수 있었으나 정보보호 책임자 및 개인정보 보호책임자의 부재와 정보보호 및 개인정보보호 관리자, 실무자 등이 관리 업무를 지원, 이행할 수 있도록 직무기술서 등을 통해 책임 및 역할을 구체적으로 정의해야 함
- 정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하여야 함
- 정보보호 및 개인정보보호 관련 조직 및 조직의 구성원간 상호 의사소통 할 수 있는 체계 및 절차를 수립·이행하여야 함

□ 개선방안

- **정보보호 및 개인정보보호 업무 수행과 관련된 조직의 특성을 고려하여 관련 책임자와 담당자의 역할 및 책임을 시행문서에 구체적으로 정의하여야 합니다.**

  정보보호 최고책임자 및 재인정보 보호책임자

정보보호, 개인정보보호 관리자 및 담당자

부서별 정보보호, 개인정보보호 책임자 및 담당자

정보보호 최고책임자	개인정보 보호책임자
정보보호 관리체계의 수립 및 관리 운영 정보보호 취약점 분석·평가 및 개선 침해사고의 예방 및 대응 사전 정보보호대책 마련 및 보안조치 설계·구현 정보보호 사전 보안성 검토 중요 정보의 암호화 및 보안서버 적합성 검토 그 밖에 정보통신망법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행	개인정보 보호 계획의 수립 및 시행 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 개인정보 처리와 관련한 불만의 처리 및 피해 구제 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 개인정보 보호 교육 계획의 수립 및 시행 개인정보파일의 보호 및 관리·감독 개인정보 처리방침의 수립·변경 및 시행 개인정보보호 관련 자료의 관리 처리목적이 달성되거나 보유기간이 경과한 개인정보의 파기 그 밖에 법에서 정한 개인정보 보호조치 등

- **정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하여야 합니다.**

  조직 내 성과지표(KPI), 목표관리(MBO), 인사평가 등 정보보호 및 개인정보보호 활동을 평가할 수 있는 방안을 마련하여 주기적으로 평가하여야 합니다.

- **정보보호 및 개인정보보호 관련 조직 및 조직의 구성원간 상호 의사소통 할 수 있는 체계 및 절차를 마련해야 합니다.**

  - 정보보호 및 개인정보보호 관련 의사소통 관리 계획

    - 의사소통 관리 계획 개요: 목적 및 범위

    - 의사소통 체계: 전사 협의체, 실무 협의체, 위원회 등 보고 및 협의체 운영방안, 참여 대상, 역할 및 책임, 주기 등

    - 의사소통 방법: 보고 및 회의(월간, 주간 보고 등), 공지, 이메일, 메신저, 정보보호 포털 등

    - 의사소통 양식: 유형별 보고서 양식, 회의록 양식 등

기준	J 회사의 정보자산 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산 별 책임소재를 명확히 정의하고 관리해야 합니다. J 회사내, 조직의 업무 특성에 따라 정보자산 분류기준을 수립해 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리해야 합니다.
확인 사항	1. 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호 대책을 정의하고 이행해야 합니다. - 기업에서는 정보자산에 대한 정책을 마련해 식별하고 목록화해서 관리해야 합니다. 또한 정보자산의 등급에 따라 취급절차를 정의하고 적절한 보안 통제를 적용합니다. - 문서자산의 경우 각 기밀, 대외비, 일반등의 문서 등급을 분류하고, 각 등급별로 생성, 저장, 이용, 파기에 대한 취급자 유의 사항을 마련해야 합니다. - 클라우드 서비스를 이용 시 클라우드 서비스 가상자원에 대한 취급절차 및 보호대책을 정의하고 이행하여야 합니다. 2. 정보자산의 분류기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별해 목록으로 관리해야 합니다. **※ 정보자산 분류 (예시)** **>자산 유형별 분류:** 서버, 데이터(DBMS), 정보처리시스템(응용프로그램), 소프트웨어, 네트워크장비, 보안시스템, PC, 정보, 설비, 시설 등 **>자산 유형별 항목(예)** - 서버: Host 명칭, 일련번호, 모델명, 용도, IP 주소, 관리부서명, 관리실무자, 관리책임자, 보안 등급 등 - 데이터: DB 명, Table 명, 개인정보 항목명(예:이름,성별,생년월일,휴대폰번호,이메일 등), 관리부서명,관리실문자,관리책임자,저장 시스템(Host 명칭),저장위치(IP 주소),보안등급 등급 - 정보시스템: 서버,PC 등 단말기, 보조저장매체,네트워크 장비,응용프로그램 등 정보의 수집,가공,저장,검색,송수신에 필요한 하드웨어 및 소프트웨어 - 보안시스템: 정보의 훼손,변조,유출 등을 방지하기 위하여 구축된 시스템으로 침입차단시스템, 침입탐지시스템,개인정보유출방지시스템 등을 포함 - 정보:문서적 정보와 전자적 정보 모두를 포함(중요정보, 개인정보 등) 3. 식별된 정보자산의 중요도를 평가할 수 있도록 기준을 수립하고 관리자 및 책임자를 지정하여 책임소재를 명확하게 하여야 합니다. - 법적 요구사항이나 업무에 미치는 영향 등 각 자산 특성에 맞는 보안등급 평가기준 결정 ※ 보안등급 산정기준 (예시) - 기밀성, 무결성, 가용성, 법적 준거성 등에 따른 중요도 평가 - 서비스 영향, 이익손실, 고객 상실, 대외 이미지 손상 등도 고려

	- 정보자산별로 책임자 및 관리자 지정하고 자산목록에 기록 - 퇴직, 전보 등 인사이동이 발생하거나 정보자산의 도입·변경·폐기 등으로 정보자산현황이 변경될 경우 정보자산별 책임자 및 담당자를 파악하여 자산목록에 반영합니다.

□ 현황과 문제점

- 정보자산의 보안등급에 따른 취급절차 및 보호 대책의 부재
- J 회사의 각 사업의 정보자산 및 개인정보 보안등급 분류 기준과 자산관리 대장 분류 기준의 부재
- 정보자산별 담당자 및 책임자를 식별하지 않고 자산목록 현행화 미흡

□ 개선방안

- **J 회사는 정보자산에 대한 정책을 마련해 식별하고 목록화해서 관리해야 합니다.**

  〉정보시스템, 정보보호시스템을 포함해 조직 및 업무 특성을 고려한 자산 분류 기준을 정의하고 서버, PC, 네트워크 장비, 침입차단시스템, 침입탐지시스템, 침입방지시스템, 게인정보 유출 방지시스템, 응용 프로그램 등 정보 수집, 가공, 저장, 검색, 송수신에 필요한 하드웨어 및 소프트웨어, 하드 카피 형태 문서 이외에 전자결제 등의 전자문서도 식별 범위에 모두 포함해 목록화해야 합니다.

  〉클라우드 서비스 이용 시 클라우드 서비스 자원의 분류기준을 수립하고 자원의 생성, 수정, 삭제의 이력관리를 위한 방안을 마련해야 합니다.

  - 다수의 리전에서 사업 별 클라우드 서비스를 이용하는 경우 분산돼 있는 가상자원을 식별하고 관리할 수 있는 방안 마련
  - 정기적으로 클라우드 서비스 가상자원의 사용 현황을 검토해 미사용 자원의 중지, 효율이 떨어지는 자원에 대한 통합 등의 수행 방안 마련

[정보자산 관리 지침] - 예시

제 1 조[정보자산의 분류]

정보자산은 유형에 따라 다음과 같이 분류해 관리한다.

구분	설명	종류
서버	사용자에게 특정 서비스를 제공하기 위한 기능의 운영체제 및 프로그램이 설치되어 있는 장비	▪ APP서버 ▪ DB서버 ▪ 개발서버 ▪ Web서버 ▪ WAS서버 등
네트워크장비	서비스 운영 및 제반 업무를 위해 설치된 네트워크 장비	▪ 라우터 ▪ L4/L3/L2 스위치 등
보안장비	서비스 보안 운영을 위한 보안 장비	▪ 방화벽 ▪ IDS ▪ IPS ▪ DDoS대응시스템 등
DBMS	업무 및 서비스 운영에 필요한 데이터 관리를 위해 대·내외적으로 사용되고 있는 Database 관리시스템	▪ Oracle ▪ MS-SQL ▪ Tibero ▪ My-SQL 등
PC	업무 수행을 목적으로 정보를 처리하는 단말기	▪ Desktop ▪ 노트북 ▪ 단말기 등
기타장비	각종 시스템 및 네트워크 장비의 운영을 지원하기 위한 장비	▪ 백업장치 ▪ 스토리지

제 2 조[자산 목록 관리]

가. 자산 유형에 정의된 정보처리시설 자산의 등록, 변경, 이관 폐기와 같은 자산관리를 위해 자산목록을 자산 관리 시스템 또는 대장에 작성에 관리해야 한다.

나. 자산목록은 자산의 변경 시 즉시 갱신해야 하며, 연 1 회 이상 자산 변경사항을 파악해 자산 목록을 갱신해야 한다.

제 2 조[정보자산 목록 작성]

정보자산을 도입하거나 새로운 자산이 생성될 때에는 다음 절차에 따라 정보자산 목록을

목록을 작성해야 한다.

1) 정보자산 책임자는 정보자산을 도입하거나 새로운 정보자산이 생성될 때 정보자산 목록 작성

2) 정보자산 관리자는 해당 정보자산 관리자에게 정보자산 목록의 작성을 요청

3) 해당 정보자산 관리자는 이 지침에서 제시한 정보자산 목록 작성 방법에 따라 양식을

작성해 정보자산 목록 작성

- 정보자산 목록 유형에 따라 자산형태, 제품명, 용도, IP, 관리자, 책임자, 관리부서, 중요도, 등급등을 포함해 작성하고 자산의 변동이 있는 경우 수시로 업데이트를 진행해 최신 상태를 유지해야 합니다.

- 식별된 정보자산의 법적 요구사항 및 업무에 미치는 영향 등을 고려해 중요도를 결정하고 보안등급을 부여해야 합니다.

〉식별된 정보자산은 자산 명, 자산번호, 모델명, 용도, 자산 별 책임자, 관리자, 관리부서, 보안등급 등이 포함되도록 목록을 작성해야 하며, 정기적으로 정보자산 현황을 조사해 정보자산 목록을 최신으로 유지해야 합니다.

※ 보안등급 산정기준 (예시)

기밀성, 무결성, 가용성, 법적 준거성 등에 따른 중요도 평가

교육서비스 영향, 회원 상실, 대외 이미지 손상 등도 고려

〉신규 도입, 변경, 폐기되는 자산 현황을 확인할 수 있도록 절차 마련

- 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호 대책을 정의하고 이에 따라 암호화, 접근통제 등 적절한 보호대책을 정의하고 이행해야 합니다.

〉임직원이 정보자산별 보안등급(기밀, 대외비, 일반 등)을 식별할 수 있도록 표시

전자문서: 문서 표시 또는 워터마킹을 통해 표시

서버 등 하드웨어 자산: 자산번호 또는 바코드 표시를 통한 보안등급 확인

- 클라우드 서비스를 이용 시 클라우드 서비스 가상자원에 대한 취급절차 및 보호대책을 정의하고 이행해야 합니다.

〉조직의 정보자산 분류기준이 클라우드 정보자산 분류에 유효한지 확인하고, 필요 시 클라우드 정보자산 분류기준을 별도로 수립

〉클라우드 서비스 제공자에 의해 서비스 형태로 제공되는 자산과 이용자에 의해 생성, 관리되는 가상 정보자산을 구분해 관리

〉클라우드 서비스의 정보자산이 누락되지 않도록 식별하고 목록을 관리할 수 있는 방법 마련

〉클라우드 서비스의 배포가 수시로 발행돼 기존 가상자원이 수시로 변경되는 경우, 이력을 관리할 수 있는 방안 마련

〉클라우드 환경에서의 정보자산에 대한 책임자 및 관리자 지정

〉클라우드 서비스 정보자산의 중요도를 평가하기 위한 기준 수립

〉동일한 종류의 정보자산이라도 서비스 지역, 서비스 모델, 구축 환경에 딸 차이가 발생할 수 있기 때문에 보안등급 평가 시 고려

- 식별된 정보자산의 중요도를 평가할 수 있도록 기준을 수립하고 관리자 및 책임자를 지정해야 합니다.

〉정보자산은 유출 시 위험도, 장애의 비즈니스 영향도, 침해 사고 발생 시 사회적으로 미치는 영향 등에 따라 중요도가 다르기 때문에 기밀성, 무결성, 가용성, 법적요구사항 등에 따라 중요도를 평가하고 보안등급을 부여해야 함 또한, 정보자산에 대한 관리책임을 강화하기 위해서 관리자 및 책임자를 명확하게 지정해야 함

〉클라우드 환경에서는 가상자원을 생성하거나 클라우드 서비스 제공자가 제공하는 서비스 형태의 자원을사용하므로 가상자원을 생성해 사용하는 경우, 자산을 식별할 수 있도록 네이밍(Naming) 규칙을 수립해 가상자원 생성 시 해당 규칙을 적용할 수 있도록 해야 함

클라우드 자원은 랜덤으로 자산정보가 생성되므로 네이밍 규칙을 적용하지 않을 경우 관리하는 데 어려움이 발생할 수 있음

클라우드 자원을 목록으로 관리하는 것이 필요한 경우 에는 상태, 가용 영역, Hostname, 용도, IP, 관리자, 책임자, 관리부서 사용 키, VPC, Subnet, 운영체제, 중요도, 보안등급, 등을 포함해 목록으로 관리할 수 있음

[인증 및 권한 관리]

기준	J 회사의 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정하고 인식시켜야 합니다.
확인 사항	1. 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한의 등록·변경·삭제에 관한 공식적인 절차를 수립·이행해야 합니다. - 정보시스템 및 개인정보처리시스템의 사용자 계정 등록·삭제(비활성화) 및 접근권한 등록·변경·삭제는 수립된 절차에 따라 사용자가 신청하고 책임자의 승인이 완료된 후 수행되어야 합니다. - 계정은 고유한 사용자 계정을 발급하고 공유 사용을 금지해야 하며 전보, 퇴직, 부서이동 등 인사이동 발생 시 지체없이 권한 회수 또는 변경 작업을 수행해야 합니다. - 사용자 계정 발급 및 접근권한 부여의 적정성 검토를 위해 정보시스템에 등록된 사용자 계정 및 접근권한 부여 현황을 기록·관리해야 합니다. - 클라우드 서비스의 경우 클라우드 서비스 관리콘솔 계정, 롤(Role) 등의 접근권한 등록·변경·삭제에 관한 절차를 추가로 포함해야 합니다. 2. 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한의 생성·등록·변경 시 직무 별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시켜야 합니다. - 개인정보 및 중요정보를 취급하는 직무 별 또는 역할별로 분류체계를 작성해 정보시스템 접근권한을 정의하고 정보시스템 및 개인정보처리시스템에 대한 접근권한은 업무 수행에 필요한 최소한으로 할당하고 최소인원에 대해 할당해야 합니다. - 개인정보처리시스템의 접근권한부여 현황, 변경 또는 말소 내역 등을 기록하고 관련 법령에 따라 보관해야 하며 개인정보 취급자의 퇴직, 계약 종결 또는 직무 변경 시 ·접근권한을 제거 또는 변경해야 합니다. - 클라우드 서비스를 이용하는 경우 관리자, 일반사용자 등 권한을 차등해서 부여할 수 있는 기능을 제공하는지 여부와 각 계정의 로그인, 로그아웃 등 행위이력을 기록하는 기능을 제공하는지 검토해야 합니다. - 사용자에게 계정 및 접근권한을 부여하는 경우 정보보호정책, 서양서 등을 통해 계정에 대한 책임은 사용자에게 있음을 명기하고 이메일, 공지, 교육 등을 통해 지속적으로 인식을 제공해야 합니다.
관련 법규	개인정보 보호법 제 29 조(안전조치의무) 정보통신망법 제 28 조(개인정보의 보호조치) 개인정보의 안전성 확보조치 기준 제 5 조(접근 권한의 관리) 개인정보의 기술적·관리적 보호조치 기준 제 4 조(접근통제)

□ 현황과 문제점

- 공식적인 사용자 등록·해지 요청 및 승인 절차를 거치지 않고 필요에 따라 권한을 부여 또는 삭제 (퇴직자의 계정 삭제 및 말소는 관리되고 있음)
- 정보시스템 또는 응용프로그램 사용자가 모든 정보에 자유롭게 접근가능한 구조
- 사용자 계정 관리 절차의 계정발급 및 접근권한 부여 현황목록, 승인 이력의 부재
- 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시키고 해당 계정에 대한 보안책임 인식 교육 필요 (단, 연 1 회 공통으로 개인정보보호 관련 교육 진행)
- J 회사의 현 업무 환경은 대면·비대면을 병행, 비대면 업무(원격근무) 시 정보보안 강화를 위한 계정관리 가이드 필요
- J 회사 임직원의 비대면 업무(원격 업무) 시, 전용 접속 환경으로 VPN(가상사설망) 이용

□ 개선방안

- **J 회사의 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하기 위하여 다음의 사항을 고려하여 공식적인 사용자 계정 및 접근권한 등록·변경·삭제·해지 절차를 수립·이행하여야 합니다.**

〉사용자 및 개인정보취급자 별로 고유한 사용자 계정 발급 및 공유 금지

〉사용자 및 개인정보취급자에 대한 계정 발급 및 접근권한 부여·변경 시 승인절차 등을 통한 적절성 검토

〉전보, 퇴직 등 인사이동 발생 시 지체없이 접근권한 변경 또는 말소(계정 삭제 또는 비활성화)

〉정보시스템 설치 후 제조사 또는 판매사의 기본 계정, 시험 계정 등은 제거하거나 추측하기 어려운 계정으로 변경

〉사용자 계정 및 접근 권한의 등록·변경·삭제·해지 관련 기록의 유지·관리 등

- **정보시스템 및 개인정보처리시스템 도입, 구축, 개발 시 접근권한을 업무 수행 목적에 따라 최소한의 범위로 차등 부여할 수 있는 기능, 계정 생성 · 변경 · 삭제, 권한부여에 대한 기록을 남길 수 있는 기능, 로그인, 로그아웃, 메뉴접근 등의 행위 이력을 남길 수 있는 기능을 제공하는지 확인해야 합니다. 특히 개인정보처리시스템은 계정생성 및 권한부여 이력을 개인정보보호법 '개인정보의 안정성 확보조치 기준 제 5 조(접근권한의 관리) 3 항'에 따라 3 년간 보관하거나 '개인정보의 안정성 확보조치 기준 제 5 조(접근권한의 관리) 3 항'에 따라 3 년간 보관하거나 '개인정보의 기술적 · 관리적 보호조치 기준 제 4 조(접근통제) 3 항'에 따라 5 년간 보관해야 합니다.**
- **정보시스템과 개인정보 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성·등록·변경 시 직무 별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하여야 합니다.**

〉정보시스템 및 개인정보처리시스템에 대한 접근권한은 업무 수행 목적에 따라 최소한의 범위로 업무 담당자에게 차등 부여

〉중요 정보 및 개인정보에 대한 접근권한은 알 필요(need-to-know), 할 필요(need-to-do)의 원칙에 의해 업무적으로 꼭 필요한 범위에 한하여 부여

〉불필요하거나 과도하게 중요 정보 또는 개인정보에 접근하지 못하도록 권한 세분화

〉권한 부여 또는 변경 시 승인절차 등을 통하여 적절성 검토 등

- 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시켜야 합니다.

〉정보보호 및 개인정보보호 정책, 서약서 등에 계정에 대한 책임과 의무를 명기(타인에게 본인 계정 및 비밀번호 공유 대여 금지, 공공장소에서 로그인 시 주의사항 등)

〉서약서, 이메일, 시스템 공지, 교육 등 다양한 방법 활용

- 비대면 업무(원격 업무) 시, 통합 인증체계 운영하여 업무용 전산환경의 모든 접속은 단일 계정으로 통합 인증을 수행합니다.

〉VPN 접속, 업무용 응용 프로그램 로그인 등의 계정을 통합 관리함으로써 사용자 접속 이력 및 행위 추적성 확보

〉계정을 공유할 수 없도록 제한하고 개별 사용자마다 구분된 권한을 부여하여 사용자별 이력 및 행위 추적성 확보

〉사용자 접속 이력, 접속 출발지 및 목적지 등을 지속적으로 모니터링하여 이상징후 탐지

- 비대면 업무(원격 업무) 시, 허가된 사용자와 단말기만이 업무망에 접근할 수 있도록 전용 접속 환경(VPN 이용)

〉VPN 접속, 서비스 접근은 기업에서 지정한 단말기만 허용하도록 설정

〉VPN 으로 접속하는 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용)를 점검할 수 있어야 함

〉VPN 으로 접속하는 사용자는 반드시 계정/비밀번호 외에 추가로 다중 인증 적용하기

〉VPN 접속 시 사내 네트워크를 통해서 외부 인터넷으로 접속하도록 트래픽 경로 단일화하여 모니터링 가시성 확보

- J 회사 사내 업무용 시스템 로그를 상시 모니터링하여 이상징후를 탐지하는 등 보안활동 강화

〉VPN 을 통해 접속된 원격 근무자는 기업 내부망에서 가지는 권한과 동일한 권한을 가지므로 내부 네트워크 망 전체의 보안 모니터링 필수

〉원격근무용 네트워크는 주소 대역을 달리하여 모니터링 용이성 확보

〉내부 업무용 서버의 보안성 강화(백신 설치, 최신 보안 업데이트, 내부 자원 모니터링) 적용

〉서버 간 불필요한 접근을 최소화하고, 필요시 계정 별 권한을 부여하여 활동범위(작업범위)를 제한하는 등 접근통제 강화

〉VPN 접속 현황 및 사용자 행위 이력 모니터링 등 이상징후 탐지 방안 확보

- J 회사 임직원의 비대면 업무 시, 영상 회의 개설 시 보안 설정 및 참석자 인증 실시

〉영상회의를 개설할 때 반드시 회의실에 입장하기 위한 암호를 설정하기

〉영상회의실은 고정주소를 사용하지 않고 개설 시점에 새로운 주소 또는 새로운 회의실 번호를 사용하기

〉영상회의 개설자는 초대자와 참석자의 일치 여부 확인

〉개설자의 노트북, 스마트폰, 태블릿 등은 최신 보안 업데이트 상태로 관리

- Microsoft 365 **사용자 계정관리**
  https://docs.microsoft.com/ko-kr/microsoft-365/enterprise/manage-microsoft-365-accounts?view=o365-worldwide#managing-accounts

기준	J 회사의 정보시스템 및 개인정보처리시스템의 사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고, 추측 가능한 식별자 사용을 제한해야 합니다. 동일한 식별자를 공유해 사용하는 경우 그 사유와 타당성을 검토해 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행해야 합니다.
확인 사항	1. 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보 취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한해야 합니다. - 정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자(아이디)를 할당해 모든 사용자의 책임추적성을 보장해야 하며, 관리자 및 특수권한 계정의 경우 추측 가능한 식별자(root, admin 등)의 사용을 제한해야 합니다. - 시스템 설치 후 정보시스템의 기본 계정은 제거 또는 추측이 어려운 계정으로 변경해야 하며, 변경이 어려운 경우 비밀번호를 변경해야 합니다. 2. 공용계정을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 하며, 책임추적성을 보장할 수 있도록 통제방안을 마련해야 합니다.
관련 법규	개인정보 보호법 제 29 조(안전조치의무) 정보통신망법 제 28 조(개인정보의 보호조치) 개인정보의 안전성 확보조치 기준 제 5 조(접근 권한의 관리) 개인정보의 기술적·관리적 보호조치 기준 제 4 조(접근통제)

□ **현황과 문제점**

- J 회사의 정보시스템 및 개인정보처리시스템의 사용자 계정은 사용자별로 구분할 수 있도록 아이디를 할당 (예: hjpark, 이름 이니셜 아이디)
- 동일한 식별자를 공유하여 사용하는 경우는 없으며, 외부에서 내부 시스템(J 회사)에 접근해야 하는 경우(외부 업체 또는 기관과의 공유계정 사용)는 MS One-Drive 에 생성한 해당 파일만 링크로 공유 및 취합
- 외부인 계정발급의 사례는 없으나, 필요시 접근권한을 제한하여 발급 가능
- 업무는 클라우드 환경의 Office365 를 활용, 직원의 접근(엑세스) 현황 확인 가능

□ **개선방안**

- 정보시스템 및 개인정보처리시스템에 대한 사용자 등록 시 사용자 및 개인정보 취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한해야 합니다.

〉J 회사의 1 인 1 계정 발급을 통해 사용자에 대한 책임추적성을 확보하고 있으며, 계정 공유 및 공용 계정 사용 제한하고 있음

〉시스템이 사용하는 운영계정은 사용자가 사용하지 못하도록 제한할 필요가 있으며 시스템 설치 후 제조사 또는 판매사의 기본계정 및 시험계정은 제거 또는 추측이 어려운 계정으로 변경해야 함

〉관리자 및 특수권한 계정의 경우 쉽게 추측 가능한 식별자의 사용을 제한할 것

- **앞으로 업무상 불가피하게 동일한 식별자를 공유하여 사용하게 될 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 합니다.**

〉업무 분장상 역할이 구분되어 관리자 계정을 공유하는 경우에도 사용자 계정을 별도로 부여하고 사용자 계정으로 로그인 후 관리자 계정으로 변경

〉유지보수 업무 등을 위하여 임시직으로 계정을 제공한 경우 업무 종료 후 즉시 해당 계정의 비밀번호를 변경

〉업무상 불가피하게 공용계정 사용이 필요한 경우 그 사유와 타당성을 검토하여 책임자의 승인을 받고 책임추적성을 보장할 추가적인 통제방안 적용

-

<table>
<tr><td>기준</td><td>J 회사의 정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용해야 합니다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행해야 합니다.</td></tr>
<tr><td>확인 사항</td><td>1. 정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제해야 합니다.
- 사용자 인증 수단 예시
<table>
<tr><th>구 분</th><th>인증 수단</th><th>비 고</th></tr>
<tr><td>지식기반</td><td>비밀번호</td><td>• 안전한 비밀번호 작성규칙 및 주기적 변경 필요
• 비밀번호 도용, 무작위 대입 공격 등에 대한 대응 필요
• 시스템 설치 시 제품 등에서 제공하는 디폴트 계정 및 비밀번호 사용정지 또는 변경 필요</td></tr>
<tr><td rowspan="3">소유 기반</td><td>인증서(PKI)</td><td>• 개인키의 안전한 보관 필요(안전한 보안매체에 보관 권고)</td></tr>
<tr><td>OTP
(One Time Password)</td><td>• OTP토큰, 모바일OTP 등 다양한 방식 존재</td></tr>
<tr><td>기타</td><td>• 스마트 카드 방식
• 물리적 보안토큰 방식 등</td></tr>
<tr><td>생체 기반</td><td>지문, 홍채, 얼굴 등</td><td>• 생체 정보의 안전한 관리 필요
※ 참고 : FIDO(Fast Identity Online)</td></tr>
<tr><td rowspan="4">기타 방식</td><td>IP 주소</td><td>• 특정 IP주소에서만 해당 아이디로 접속할 수 있도록 제한하는 방식</td></tr>
<tr><td>MAC 주소</td><td>• 단말기의 MAC주소를 기반으로 등록된 단말기에서만 접속할 수 있도록 제한하는 방식</td></tr>
<tr><td>기기 일련번호</td><td>• 특정 PC 또는 특정 디바이스(스마트폰 등)에서만 접속할 수 있도록 제한하는 방식</td></tr>
<tr><td>기타</td><td>• 위치 정보 등</td></tr>
</table>
- 계정 도용 및 불법적인 인증시도 통제방안 예시
<table>
<tr><th>구 분</th><th>설명</th></tr>
<tr><td>로그인 실패횟수 제한</td><td>• 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 접근 제한
※ 개인정보의 안전성 확보조치 기준 제5조제6항</td></tr>
<tr><td>접속 유지시간 제한</td><td>• 접속 후, 일정 시간 이상 업무처리를 하지 않은 경우 자동으로 시스템 접속 차단 (Session Timeout 등)
※ 개인정보의 안전성 확보조치 기준 제6조제5항
※ 개인정보의 기술적·관리적 보호조치 기준 제4조제10항</td></tr>
<tr><td>동시 접속 제한</td><td>• 동일 계정으로 동시 접속 시 접속차단 조치 또는 알림 기능 등</td></tr>
<tr><td>불법 로그인 시도 경고</td><td>• 해외 IP주소 등 등록되지 않은 IP주소에서의 접속 시 차단 및 통지
• 주말, 야간 접속 시 문자 알림
• 관리자 등 특수 권한 로그인시 알림 등</td></tr>
</table>
2. 인터넷 등 정보통신망을 통해 외부에서 개인정보시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증수단 또는 접속수단을 적용해야 합니다.
- 안전한 인증수단: 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등</td></tr>
</table>

	- 안전한 접속수단: 가상사설망(VPN), 전용망 등
관련 법규	개인정보 보호법 제 29 조(안전조치의무) 정보통신망법 제 28 조(개인정보의 보호조치) 개인정보의 안전성 확보조치 기준 제 5 조(접근 권한의 관리), 6 조(접근통제) 개인정보의 기술적·관리적 보호조치 기준 제 4 조(접근통제)

□ 현황과 문제점

- 현재까지 계정 도용 및 불법적인 인증시도의 사례 없음

- J 회사의 각 사업 정보나 데이터를 원드라이브에 저장하고 MS 시스템 상 다단계 인증을 거쳐 로그인을 할 수 있도록 설정

- J 회사의 정보시스템 및 개인정보처리시스템 로그인 실패 시 해당 아이디가 존재하지 않거나 비밀번호가 틀림을 표시해 주고 있으며, 내부 정보시스템의 로그인 실패 횟수 제한은 설정하였으나 WEB 을 통한 접근 시 로그인 실패 횟수 제한 확인 불가

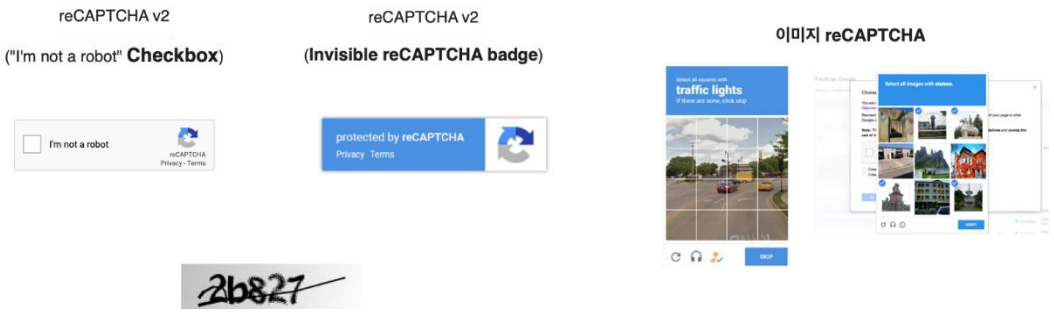
- J 회사의 정보시스템 및 개인정보처리시스템의 불법 로그인 시도 시 경고 알림 설정

- 동시 접속 제한 및 접속 유지시간의 제한 확인 필요

□ 개선 방안

- J 회사의 정보시스템 및 개인정보처리시스템에 대한 접근은 MS 시스템 상 다단계 인증을 거쳐 로그인을 할 수 있도록 설정, 안전한 인증수단을 확인 점검하여 통제해야 합니다.

〉인증 시도가 실패했을 경우 실패 시마다 경고문구를 삽입하고 특정 횟수가 초과된 경우에는 비인가자의 로그인 시도를 차단하기 위한 캡챠 등으로 추가 인증할 수 있도록 제한해야 합니다.



〉캡챠의 경우 해킹 사례가 다수 확인되고 있기 때문에 개인정보 취급자가 불가피하게 외부에서 개인정보처리시스템에 접속하는 경우, 개인정보처리시스템을 외부에 오픈할 수밖에 없는 경우, 클라우드 관리콘솔 로그인의 경우, 그 밖에 회사에서 중요하다고 생각하는 데이터를 보유한 정보시스템에 로그인하는 경우 2Factor 인증 등 강화된 인증 방식 사용해야 함

- **공개 인터넷망을 통해 접속을 허용하는 개인정보처리시스템의 경우 개인정보보호법의 '개인정보의 기술적 · 관리적 보호조차 기준(고시)' 제 4 조(접근통제)에 따라 아이디, 비밀번호 인증 이외의 강화된 인증수단(OTP, 공인인증서, 전화인증 등)을 적용해야 하며 VPN 및 전용망을 사용해 접속 시 인증정보가 유출되는 것을 보호해야 합니다.**

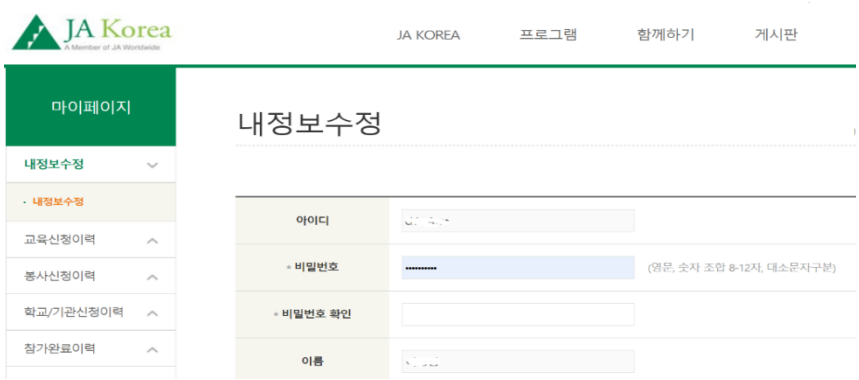
.>VPN 및 전용망을 사용해 연결된 경우에도 아이디, 비밀번호 인증만 사용할 경우 키로커 등의 악성코드로 인해 인증정보가 유출될 수 있기 때문에 2Factor 인증 등 강화된 인증 방식을 추가로 적용해야 함

<table>
<tr><td>기준</td><td>법적 요구사항, 외부 위협요인 등을 고려해 J 회사의 정보시스템 사용자 및 고객, 회원 등 정보서비스 이용자가 사용하는 비밀번호 관리절차를 수립·이행해야 합니다.</td></tr>
<tr><td>확인 사항</td><td>1. 사용자, 관리자 및 개인정보취급자가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 관리절차 및 작성규칙을 수립·이행해야 합니다.
- 비밀번호 작성규칙 예시(불가피한 경우를 제외하고는 시스템적으로 강제화 필요)
<table><tr><th>구 분</th><th>내 용</th></tr><tr><td>조합 규칙 적용</td><td>• 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상
• 또는, 영문, 숫자, 특수문자 중 3종류 이상을 조합하여 최소 8자리 이상</td></tr><tr><td>변경주기 설정</td><td>• 비밀번호 유효기간을 설정하여 반기별 1회 이상 변경</td></tr><tr><td>추측하기 쉬운 비밀번호 설정 제한</td><td>• 연속적인 숫자, 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호 사용 제한 권고</td></tr><tr><td>동일한 비밀번호 재사용 제한</td><td>• 비밀번호 변경 시 이전에 사용한 비밀번호 재사용 제한 권고</td></tr></table>- 비밀번호 관리절차 예시
· 시스템 도입 시 설정된 초기 또는 임시 비밀번호의 변경 후 사용
· 비밀번호 처리(입력, 변경) 시 마스킹 처리
· 종이, 파일, 모바일기기 등에 비밀번호 기록·저장을 제한하고 부득이하게 기록·저장해야 하는 경우 암호화 등의 보호대책 적용
· 침해사고 발생 또는 비밀번호의 노출 징후가 의심될 경우 지체없이 비밀번호 변경
· 비밀번호 분실 등에 따른 재설정 시 본인확인 절차 수행
· 관리자 비밀번호는 비밀등급에 준하여 관리 등

2. 정보주체(이용자)가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 수립·이행해야 합니다.
- 사용자 및 개인정보취급자 비밀번호 작성규칙을 참고하되, 서비스의 특성 및 민감도 등을 고려하여 적절한 수준에서 비밀번호 작성규칙 적용
- 비밀번호 분실, 도난 시 본인확인 등을 통한 안전한 재발급 절차 마련 등</td></tr>
<tr><td>관련 법규</td><td>개인정보 보호법 제 29 조(안전조치의무)
정보통신망법 제 28 조(개인정보의 보호조치)
개인정보의 안전성 확보조치 기준 제 5 조(접근 권한의 관리)
개인정보의 기술적·관리적 보호조치 기준 제 4 조(접근통제)</td></tr>
</table>

□ 현황과 문제점

- MS 의 비밀번호 정책을 J 회사의 정보시스템 계정에 반영
- 시스템 도입 시 설정된 초기 또는 임시 비밀번호의 변경 후 사용, 비밀번호 처리(입력, 변경) 시 마스킹 처리, 침해사고 발생 또는 비밀번호의 노출 징후가 의심될 경우 지체없이 비밀번호 변경, 비밀번호 분실 등에 따른 재설정 시 본인확인 절차 수행



- 이카운트, 시프티, MS Office 365 등 외부업체의 시스템을 사용하고 있으며 비밀번호는 해당업체의 규정에 따라 관리되고 있음

- 비밀번호의 변경주기는 정해진 규칙이 없음

- 비대면 근무(원격 근무) 환경 시, 전체 근무자 대상 비밀번호 보안 가이드 및 공지 권고

□ 개선방안

- **비밀번호의 경우 서버, 네트워크, 정보보호솔루션, 응용시스템 등 사용하고 있는 모든 정보시스템에 공통적으로 적용할 수 있도록 정책을 수립하고 수립된 정책은 불가피한 경우를 제외하고는 시스템에서 강제화해야 한다. 또한, IT 기기의 성능이 빠르게 향상됨에 따라 적용된 비밀번호 알고리즘이 빠르게 깨질 가능성도 증가하기 때문에 정보시스템의 중요도에 따라 법률에서 요구하는 기준보다 더 강화된 수준의 비밀 번호를 적용하는 것도 고려할 수 있습니다.**

- Microsoft 365 권장 암호 정책
  https://docs.microsoft.com/ko-kr/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

- **이용자의 비밀번호는 서비스의 특성을 고려해 비밀번호 작성규칙을 적용하고 이용자가 비밀번호를 분실한 경우에는 본인확인(공인 인증, 이메일 인증, SMS 인증, 가입 시 질문, 응답 등) 등을 통해 안전하게 재발급 받을 수 있도록 해야 합니다.**

  〉비밀번호 작성규칙 예시(불가피한 경우를 제외하고는 시스템적으로 강제화 필요)

구 분	내 용
조합 규칙 적용	• 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 • 또는, 영문, 숫자, 특수문자 중 3종류 이상을 조합하여 최소 8자리 이상
변경주기 설정	• 비밀번호 유효기간을 설정하여 반기별 1회 이상 변경
추측하기 쉬운 비밀번호 설정 제한	• 연속적인 숫자, 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호 사용 제한 권고
동일한 비밀번호 재사용 제한	• 비밀번호 변경 시 이전에 사용한 비밀번호 재사용 제한 권고

〉이용자(정보주체)의 비밀번호 작성 규칙은 사용자(서비스 제공자)의 비밀번호 작성 규칙과 동일하게 적용하는 것이 좋음

〉해킹 사고가 빈번하게 발생하는 인터넷 서비스나 게임 서비스의 경우 공인인증서를 강제화 하거나 전화인증, OTP 등을 이용자가 선택 사용할 수 있도록 제공해서 아이디, 비밀번호 인증에서 발생할 수 있는 문제점을 보완하고 있음

- **비밀번호 변경주기를 유효기간을 설정하여 반기 별 1 회 이상 변경하도록 합니다.**

- **비대면 근무(원격근무) 환경 시, 근무자의 비밀번호 보안 가이드를 공지해야 합니다.**

〉최소 8 자 이상으로 대소문자, 숫자, 특수문자 중 2 종류 이상을 조합한 강력한 암호 사용 필수

〉특정 시간 동안 PC 를 사용하지 않는 경우 비밀번호 8 자리가 부여되는 화면보호기 장치를 활성화해야 함

〉자리를 비울 땐 장비가 완전히 로그아웃 되도록 설정하는 것이 권장

〉업무에 사용하는 계정은 개인이 일반적으로 사용하는 계정과 반드시 구분

〉단말기의 보안 수준에 상관없이 브라우저에 암호를 자동 저장하지 않기

〉카페, 야외와 같은 개방된 환경에서는 비밀번호가 주변에 노출될 수 있으므로 가능한 전용 공간확보

기준	J 회사의 정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위해 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별해 통제해야 합니다.
확인 사항	1. 관리자 권한 등 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하여야 합니다. - 정보시스템 관리, 개인정보 및 중요정보 관리 등 특수목적을 위한 계정 및 권한 유형 정의 ※ 특수 권한 (예시) · 관리자 권한(Root, Administrator, admin, sys, system, sa 등 최상위 권한) · 배치프로그램 실행이나 모니터링을 위하여 부여된 권한 · 보안시스템 관리자 권한 · 계정 생성 및 접근권한을 설정할 수 있는 권한 등 - 특수 계정 및 권한이 필요한 경우 공식적인 절차에 따라 신청 및 승인이 이루어질 수 있도록 '특수 계정·권한 발급·변경·해지 절차'를 수립·이행 - 특수 계정·권한을 최소한의 업무 수행자에게만 부여할 수 있도록 일반 사용자 계정·권한발급 절차보다 엄격한 기준 적용(임원 또는 보안책임자 승인 등) 2. 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하는 등 통제절차를 수립·이행하여야 합니다. - 특수권한자 목록 작성·관리 - 특수권한자에 대해서는 예외조치 최소화, 모니터링 강화 등의 통제절차 수립·이행 - 정보시스템 유지보수 등 외부자에게 부여하는 특수권한은 필요시에만 생성, 업무 종료 후에는 즉시 삭제 또는 정지하는 절차를 적용 - 특수권한자 현황을 정기적으로 검토하여 목록 현행화
관련 법규	개인정보 보호법 제 29 조(안전조치의무) 정보통신망법 제 28 조(개인정보의 보호조치) 개인정보의 안전성 확보조치 기준 제 5 조(접근 권한의 관리) 개인정보의 기술적·관리적 보호조치 기준 제 4 조(접근통제)

□ **현황과 문제점**

- J 회사의 최소한의 인원에게만 부여될 수 있는 관리자 권한 및 특수권한의 공식적인 승인 및 승인절차의 부재

- 현 J 회사의 관리자 권한 및 특수권한은 경영기획팀 내 담당자만 부여받음

- 특수 목적을 위해 부여한 계정은 목록화 하진 않고 별도로 관리함

- 특수권한자 현황을 정기적으로 검토하여 목록 현행화 필요

□ **개선방안**

- **관리자(root, admin 등) 및 특수 권한(배치나 모니터링을 위해 부여받은 권한, 계정 및 접근 설정 권한 등) 할당 시 책임자의 승인을 받고 사용자를 최소한으로 제한해야 합니다.**

- **특수목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리, 예외조치 최소화, 모니터링 강화 등의 통제절차를 마련해야 합니다.**

  〉특수권한자 목록 작성·관리

  〉특수권한자에 대해서는 예외조치 최소화, 모니터링 강화 등의 통제절차 수립·이행

  〉특수권한자 현황을 정기적으로 검토하여 목록 현행화

- **외부자에게 부여하는 계정은 한시적으로 부여한 계정 등 특수 목적을 위한 계정도 별도의 목록으로 관리하고 업무 목적이 달성된 경우에는 즉시 삭제 또는 권한을 회수하는 등의 통제절차를 마련해야 합니다.**

  〉정보시스템 유지보수 등 외부자에게 부여하는 특수권한은 필요시에만 생성, 업무 종료 후에는 즉시 삭제 또는 정지하는 절차를 적용

- **클라우드 서비스 이용 시, 클라우드 관리콘솔의 최고 사용자 권한은 모든 가상자원에 대한 생성·변경·삭제가 가능하기 때문에 사용을 제한하고 일부 권한을 부여한 계정을 생성해서 사용해야 합니다.**

  〉Root, admin 등의 관리자 계정은 MFA(2factor 인증)를 적용해 보호

  〉 Access Key 를 사용할 경우, 암호화 키 생성·삭제·변경 절차를 수립하고 주기적으로 Access Key 교체

기준	J 회사의 정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토해 적정성 여부를 점검해야 합니다.
확인 사항	1. 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남기고 사용자 계정 및 접근권한의 적정성 검토 기준, 검토주체, 검토방법, 주기 등을 수립해 정기적 검토를 이행하여야 합니다. - 사용자 계정 및 접근권한에 대한 내역은 책임추적성을 확보할 수 있도록 필요한 사항을 모두 포함하여 기록(계정 및 접근권한 신청정보, 승인정보, 등록정보, 정보) - 접근권한 기록은 법적 요구사항 등을 반영하여 일정기간 동안 보관 [개인정보 보호법]에 따른 개인정보처리자: 최소 3 년간 보관 [정보통신망법]에 따른 정보통신서비스 제공자 등: 최소 5 년간 보관 2. 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토주제, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하여야 합니다. - 접근권한 검토 주체, 방법, 기준 주기(최소 분기 1 회 이상 권고), 결과보고 등 검토 절차 수립 ※ 접근권한 부여의 적정성 검토 항목 (예시) · 공식적인 절차에 따른 접근권한 부여 여부 · 접근권한 분류체계의 업무목적 및 보안정책 부합 여부 · 접근권한 승인자의 적절성 · 직무변경 시 기존 권한 회수 후 신규 업무에 대한 적절한 권한 부여 여부 · 업무 목적 외 과도한 접근권한 부여 여부 · 특수권한 부여·변경·발급 현황 및 적정성 · 협력업체 등 외부자 계정·권한 발급 현황 및 적정성 · 접근권한 신청·승인 내역과 실제 접근권한 부여 현황의 일치 여부 · 장기 미접속자 계정 현황 및 삭제(또는 잠금) 여부 · 휴직, 퇴직 시 지체없이 계정 및 권한 회수 여부 등 3. 접근권한 검토 결과 접근권한 과다 부여, 권한부여 절차 미준수, 권한 오·남용 등 문제점이 발견된 경우 그에 따른 조치절차를 수립·이행하여야 합니다. - 접근권한 검토 후 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지 - 유사한 문제가 반복될 경우 근본 원인 분석 및 재발방지 대책 수립
관련 법규	개인정보 보호법 제 29 조(안전조치의무) 정보통신망법 제 28 조(개인정보의 보호조치) 개인정보의 안전성 확보조치 기준 제 5 조(접근 권한의 관리) 개인정보의 기술적·관리적 보호조치 기준 제 4 조(접근통제)

□ **현황과 문제점**

- J 회사는 정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정 및 접근권한의 검토 기준 및 절차의 부재

- J 회사는 정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정 및 접근권한의 검토 이력 부재

- 현재 J 회사는 정보시스템과 개인정보 및 중요정보에 접근하는 사용자의 접근권한 과다 부여, 권한부여 절차 미준수, 권한 오·남용 등 문제점의 발견 등의 해당사례 없음

- 위의 사례에 대한 구체적인 조치절차를 수립하고 이행한 사례는 없지만, 직무변경, 퇴직 등의 발생시 접근권한을 제한함

□ **개선방안**

- 사용자 계정 및 접근권한에 대한 책임추적성을 확보할 수 있도록 신청자, 신청일시, 목적, 사용기간, 승인자, 승인일시, 접근권한 부여자, 부여일시 등을 빠짐없이 남겨야 합니다.

〉필요한 사항

-계정 . 접근권한 신청정보: 신청자 또는 대리신청자, 신청일시, 신청목적, 사용기간 등

-계정 . 접근권한 승인정보: 승인자, 승인 또는 거부 여부, 사유 및 일시 등

-계정 . 접근권한 등록정보: 등록자, 등록일, 등록방법(결재시스템 연동, 수작업 등록 등)

-계정 . 접근권한 정보: 대상 시스템명, 권한 명, 권한 내역

- 접근권한 기록은 법적 요구사항 등을 반영하여 일정기간 동안 보관하여야 합니다.

[개인정보 보호법]에 따른 개인정보처리자는 최소 3 년간 보관,

[정보통신망법]에 따른 정보통신서비스 제공자 등: 최소 5 년간 보관

- 모든 정보시스템(서버, 네트워크, 정보보호솔루션, 응용시스템, 클라우드 관리콘솔 등)에 생성된 계정 및 부여된 권한에 개해서는 검토 기준, 검토주체, 검토방법, 주기 등을 수립해 정기적으로 검토하고 검토 결과를 최고책임자에게 보고해야 합니다.

〉한 담당부서에서 모든 시스템에 대한 검토를 수행하는 것은 서비스를 상세하게 알지 못하기 때문에 권한의 과도한 부여 여부를 확인하는 데 한계가 있습니다 그렇기 때문에 아래의 검토 기준을 마련해 각 정보시스템 담당자에게 교육을 수행하고 정기적으로 검토를 수행하는 것이 좋습니다.

※ 접근권한 부여의 적정성 검토 항목 (예시)

- 공식적인 절차에 따른 접근권한 부여 여부
- 접근권한 분류체계의 업무목적 및 보안정책 부합 여부
- 접근권한 승인자의 적절성
- 직무변경 시 기존 권한 회수 후 신규 업무에 대한 적절한 권한 부여 여부
- 업무 목적 외 과도한 접근권한 부여 여부
- 특수권한 부여·변경·발급 현황 및 적정성
- 협력업체 등 외부자 계정·권한 발급 현황 및 적정성
- 접근권한 신청·승인 내역과 실제 접근권한 부여 현황의 일치 여부
- 장기 미접속자 계정 현황 및 삭제(또는 잠금) 여부
- 휴직, 퇴직 시 지체없이 계정 및 권한 회수 여부 등

〈접근권한 부여의 적정성 검토 항목〉

- 접근권한 검토 결과 권한의 과다 부여, 오남용 등 의심스러운 상황이 발견된 경우, 소명요청 및 부여과정 등의 오류 원인을 분석하고 접근권한을 변경 적용해야 합니다. 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지하고 문제가 반복되지 않도록 재발방지 대책을 마련해야 합니다.