1.1 ~ 1.3

국내에서 진행하는 ISMS-P 인증에 대해 서술하고 KoreaIT 에서의 보안침해사고 발생 시 책임 추적을 위하여 감사 로그 파일을 확보할 수 있도록 설계되어야 하는데 이 때 5가지 이상 서술하시오.

<ISMS-P>

ISMS-P란 정보보호 관리 체계(ISMS)와 개인정보보호 관리 체계(PIMS) 인증을 정보보호 및 개인정보보호 관리 체계(ISMS-P)로 통합한 것이다.
인증 대상으로는 일정 규모 이상의 정보통신서비스 제공자 및 민간기업 등으로 목적은 정보보호 및 개인정보 보호 활동이 인증 기준에 적합한지 평가하여, 조직의 정보보호 수준을 객관적으로 검증하고 신뢰성을 확보하기 위함이다.
평가 기준으로는 정보보호 정책, 위험 관리, 정보자산 보호 등 관리적,기술적,물리적 보호조치 기준으로 평가한다.

<감사 로그 파일 확보 설계>

1) 사용자 및 관리자의 접속 기록 (로그인 및 로그아웃)
   → 로그인 시각, IP 주소 등 세부 정보를 포함하여 이상 행위 식별에 활용됨

2) 사용자 권한 부여, 변경, 말소 기록
   → 권한 변경 이력을 통해 부적절한 접근 권한 설정 여부를 점검할 수 있음

3) 정보시스템 시작 및 중지 기록
   → 계획되지 않은 시스템 종료나 재부팅은 침해 가능성의 단서가 될 수 있음

4) 특수 권한으로의 접근 기록
   → root, 관리자 계정 등 고위험 계정의 활동은 별도로 집중 관리해야 함

5) 주요 업무 관련 행위에 대한 로그 등
   → 개인정보 열람, 삭제 등 민감 행위는 책임 추적을 위해 필수적으로 기록됨

2.1 ~ 2.3

KorealT 보안 인증 심사를 위해 제출해야 되는 서류 4가지 이상 서술하고 ISMS-P 보안인증의 일반적인 심사 주기에 대해 서술하시오

<보안 인증 심사를 위해 제출해야 되는 서류>

(1) 정보보호 관리 체계 인증 신청서
(2) 정보보호 관리 체계 명세서
(3) 정보보호 관리 체계의 범위 정의서
(4) 주요 정보통신 설비의 목록과 시스템 구성도
(5) 정보보호 관리 체계 수립. 운영 방법 및 절차
(6) 정보보호 관리 체계 관련 주요 문서 목록
(7) 국내외 품질경영 체제 인증서 취득 명세
(8) 사업자등록증(또는 고유 번호증)

<ISMS-P 보안인증의 일반적인 심사 주기>

최초 인증 유효기간 : 3년
사후 심사 : 매년 1회 실시
갱신 심사 : 3년 주기로 재평가

3.1 ~ 3.3

인증 심사 시 작성하는 서류 중 보안서약서와 윤리강령에 대해 서술하고 정보보호관리체계 심사 항목 중 개인정보 처리 단계별 요구사항을 나열하시오.

<보안서약서와 윤리강령>

보안서약서 : 인증 심사 관련 법규 사항 준수에 대한 사항을 서약. 입사 시, 또는 외부 용역 계약 체결 시에 작성하며, 정보 자산에 대한 기밀 유지, 무단 유출 방지, 적절한 사용 등에 대해 책임을 약속함

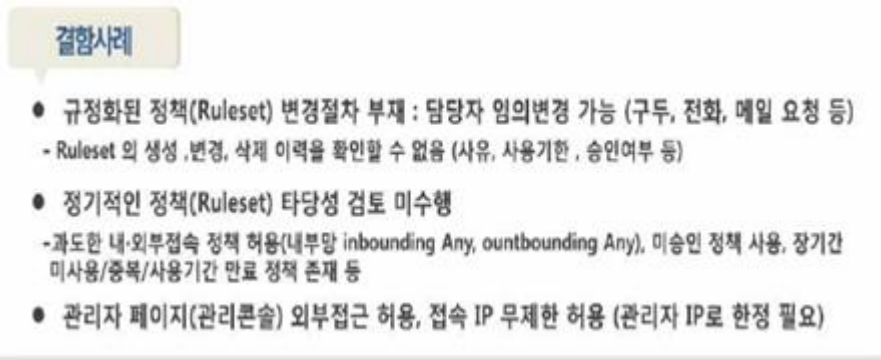
윤리강령 : 인증 심사를 공정하게 수행하고 금품이나 향을을 제공받지 않겠다는 서약. 정보보호뿐 아니라 업무의 공정성, 성실성, 책임성을 강조하며, 정보보호 사고 예방과 조직 신뢰도 확보에 기여함

<개인정보 처리 단계별 요구사항>

1) 개인정보 수집 시 보호조치
2) 개인정보 보유 및 이용 시 보호조치
3) 개인정보 제공 시 보호조치
4) 개인정보 파기 시 보호조치
5) 정보주체 권리보호

4.1 ~ 4.3

현장 심사 시 아래와 같이 보안시스템 운영 결함사례 발생 시 조치사항에 대해 서술하고 결함 사항에 대한 조치 일정에 대해 서술하시오.



<조치사항>

- 1번 항목

1) 정책 변경 절차 수립 및 문서화 - 정책 생성, 변경, 삭제 시 반드시 사유, 승인자, 승인일, 사용기한 등을 포함한 변경 요청서를 작성하도록 규정화

2) 변경 이력 관리 시스템 도입 - 정책 변경 시점, 변경자, 변경내용, 승인여부를 기록할 수 있는 로그 시스템 구축

3) 승인 절차 강화 - 변경 요청에 대해 담당 관리자 외 별도의 승인 권한자 검토 및 승인을 필수화

- 2번 항목

1) 정책 정기 검토 계획 수립 - 월간 또는 분기별로 정책의 타당성, 사용 현황 검토를 정례화

2) 자동화 도구 활용 - 정책 분석 및 비효율 정책 식별을 위한 자동화 도구 도입 검토

- 3번 항목

1) 접속 IP 제한 정책 적용 - 관리자 페이지 접근을 내부 관리자 IP 또는 VPN 접속 IP 등으로 엄격히 제한

2) 접속 로그 및 모니터링 체계 강화 - 관리자 접속 로그 기록 및 이상 접속 시 경고 체계 구축

<조치 일정>

구분	주요 작업 내용	담당부서
1단계 (1~2주)	정책 변경 절차 수립 및 문서화	보안담당팀, 시스템운영팀
	관리 IP 제한 정책 설계 및 시행	
2단계 (3~4주)	변경 이력 관리 시스템 구축 및 적용	시스템운영팀
	관리자 페이지 IP 제한 적용 완료	
3단계 (5~6주)	정책 정기 검토 프로세스 수립 및 시행	보안담당팀
	정책 자동화 도구 도입 검토 및 시범 운영	
4단계 (7주 이후)	정기적인 정책 검토 및 보고	보안담당팀, 감사팀
	접속 로그 모니터링 및 감사 체계 운영	

5.1 ~ 5.3

KorealT의 정보보호관리체계인증을 마무리 하였다고 가정할 때 사후 심사와 갱신 심사에 대해간략히 서술하고 보안인증 심사 후 인증서 발급에 대해 간략히 서술하시오.

<사후 심사 및 갱신 심사>

1) 사후 심사
   - 인증서 유효기간 동안 정기적으로 실시되는 심사로, 보통 연 1회 시행
   - 인증 받은 정보보호관리체계가 지속적으로 운영되고 있는지 점검
   - 개선 사항 및 미비점에 대해 확인하고 시정 조치 요구 가능

2) 갱신 심사
   - 인증서 만료 전에 실시하는 심사로, 보통 3년마다 시행
   - 기존 인증 범위와 체계가 최신 기준과 법규에 부합하는지 종합적으로 평가
   - 갱신 심사를 통과해야 인증서 연장이 가능하며, 미통과 시 인증 취소될 수 있음

<인증서 발급>

1) 인증서 발급
   -심사 완료 후 적합 판정을 받으면 인증기관에서 공식 인증서 발급
   - 인증서에는 인증 대상, 범위, 유효기간 등이 명시되며, 조직의 보안 수준을 대외적으로 증명하는 문서
   - 인증서 발급 후에도 사후 심사와 갱신 심사를 통해 지속적인 관리가 필요