1. 개요

본 보안 가이드라인은 미디어 산업군에 속하는 기업의 클라우드 전환에 따른 보안상 주안점 정리를 통해 과도기적 혼란 방지와 보안사고 예방의 목적에서 작성되었다. ISO/IEC 27001:2022를 기반으로 하며, ISO/IEC 27002의 통제조건 및 클라우드 환경에서의 정보보안을 위한 ISO/IEC 27017, ISO/IEC 27018 표준의 내용을 통합하였다.

기업의 정보보호 조직 구성부터 자산/정보 관리, 인적 및 물리적 보안. 통신 및 운영 관리에 이르기까지 기업 내부의 보안 정책 수립을 위해 클라우드 보안 전반의 프로세스에 대한 지침을 제공한다. 해당 내용을 바탕으로 CSP에서 클라우드 보안 핵심 가치로 주장하는 5Epics(인증/인가, 로깅/모니터링, 경계 보안, 암호화, 사고대응)를 충족할 수 있도록 설계하였다.

본 가이드를 기반으로 기업은 정보보안 관리 시스템의 범위를 고려하여 보안 정책을 설계해야 하며, 해당 정책에는 내부 시스템과 클라우드 환경 간의 상호작용, 그리고 위험관리가 포함되어야 한다. 또한 보안 정책은 문서화하여 정책서 기반의 소통 및 사용이 적절하게 가능하도록 조치를 취하여야 한다.

2. 조직 보안

본 조직 보안 목차는 미디어 기업의 정보보호 정책 수립을 위한 핵심 요소에 중점을 두어, 조직적 차원에서 고려해야 하는 보안상 주안점을 정리하고 있다. 조직 내에서의 보안 역할과 책임에 대한 명확한 정의, 권한 관리를 통한 접근 제어, 미디어 기업의 가장 큰 자산인 컨텐츠 관리 및 공급망에서의 보안 전략, 보안 사고에 대한 체계적인 증거 관리 및 대응 방안을 포함하고 있다. 이를 통해 조직은 보안에 대한 동일한 목적성을 갖고 체계적인 보안 문화 구성 및 실행의 기반을 마련할 수 있다.

A. 보안 역할과 책임

미디어 기업이 클라우드를 도입함에 있어 얻고자 하는 가장 큰 이점은 유연한 유통망과 사용자 접근성일 것이다. 하지만 클라우드 환경으로의 전환에 따른 기존의 데이터 저장 및 접근 방식, 종사자의 역할에서 변화가 발생하게 되기에 과도기적 혼란이 발생할 수 있다. 따라서 ISO/IEC 27001 인증 기준에 따라 정보보호 관리 시스템의 구축과 운영에 대한 전반적인 기준을 제시하고자 한다.

보안 역할과 책임 부분에 있어 주요 보안 지표는 다음과 같다.

1. 정책 및 승인

- 정보 보안 정책 및 특정 주제의 정책은 정의되어야 하며, 관리진에 의해 승인되어야 함.
- 정책은 게시되고, 관련 이해당사자에게 전달되어야 하며, 계획된 간격으로 또는 중요한 변화가 있을 때마다 검토되어야 함.

2. 역할 및 책임의 정의

- 조직의 필요에 따라 정보 보안 역할 및 책임을 정의하고 할당해야 함.
- 충돌하는 의무와 책임 영역은 분리되어야 하며, 모든 직원은 조직의 정보 보안 정책 및 절차를 준수해야 함.

3. 관계자 및 연락처 확립

- 조직은 관련 관계자 및 권한자와의 연락을 확립 및 유지해야 하며, 특정 관심 그룹이나 보안 포럼과의 연락도 유지되어야 함.

4. 신원 관리

- 신원의 전체 수명 주기를 관리해야 하며, 인증 정보의 할당과 관리는 관리 과정에 의해 효과적으로 제어되어야 함.

5. 클라우드 서비스 관리

- 클라우드 서비스의 획득, 사용, 관리, 종료를 위한 프로세스를 조직의 정보 보안 요구사항에 따라 확립해야 함.
- 중단 동안 정보 보안을 유지하는 계획도 필요함.

6. 법적 및 규제 준수

- 정보 보안과 관련된 법적, 통계적, 규제적 및 계약상 요구사항은 식별되고 문서화되어야 하며, 정기적으로 검토되어야 함.

7. 보안 정책 준수 검토

- 정보 보안과 관련된 법적, 통계적, 규제적 및 계약상 요구사항은 식별되고 문서화되어야 하며, 정기적으로 검토되어야 함.

8. 정보 처리 시설 운영 절차

- 정보 처리 시설의 운영 절차는 문서화되어야 하며, 필요한 직원에게 제공되어야 함.

9. 클라우드 서비스 사용자의 역할과 책임

- 클라우드 서비스 사용자는 클라우드 보안 정책을 정의하고 자신의 역할과 책임을 인식해야 함.
- 장애 처리 절차에 대한 문서화도 필수로 수행되어야 함.

이에 대한 세부 정책 예시는 다음과 같다.

보안 역할과 책임		
정책 조항	**이행 지침**	**정책 예시**
보안 정책 (ISO/IEC27002 5.15.4 5.23 5.31 5.36 ISO/IEC27017 5.1.1)	정보보안 정책 수립은 정의, 관리자의 승인의 절차를 거쳐 게시되어야 하며, 관련 이해당사자에게 전달되어 인정받는 절차가 필요함. 클라우드 서비스 이용자의 경우 클라우드 관련 보안 정책의 위험 수준이 기타 자산에 대한 정보보안 위험 수준과 일치해야 하며, 클라우드 서비스의 특성(CSP 의 데이터 접근, 데이터 저장의 물리적 위치, 클라우드 상의 자원 할당 등)을 고려하여 정책이 정의되어야 함. 클라우드 서비스 이용을 위하여 클라우드 서비스 획득, 사용, 관리 및 종료를 위한 프로세스가 정의되어야 함. 정보보안 정책 내에는 법적, 통계적, 규제적 및 계약 상의 요구사항이 반영되어야 함. 해당 정책은 정기적으로, 중요한 변화가 감지될 때마다 독립적인 검토 절차를 지켜야 함.	미디어 기업의 정보보안 정책은 산업 특성을 고려한 내부 팀 간 워크샵을 통해 개발됨. 중요한 콘텐츠와 기밀성을 고려하여 관리자의 승인 전에 직원들의 의견을 수렴하고, 외부 스테이크홀더들과의 소통이 요구됨. 클라우드 보안 정책은 미디어 기업의 역동적인 데이터 환경을 고려하여 개발되어야 하기에 미디어 파일에 대한 접근 권한과 송수신 시의 암호화, 그리고 클라우드 서비스 제공업체와의 강력한 협력 관계를 구축하는 방법이 정책에 반영되어야 함. 실시간 콘텐츠 업로드 프로세스, 권한 관리 및 모니터링, 그리고 클라우드에서의 빠른 데이터 회복 절차가 프로세스에 명시되어야 함. 미디어 기업의 정보보안 정책은 산업 특유의 법적 요구와 규제에 부합하도록 미디어 자산의 라이선스 관리, 개인정보 보호법 준수, 그리고 클라우드 제공업체와의 강화된 계약 및 협력이 정책에 포함됨.
역할 및 책임 (ISO/IEC27002 5.2 5.3 ISO/IEC27027 6.3.1)	조직의 필요에 따라 정보 보안 역할 및 책임을 정의하고 할당해야하며, 충돌하는 의무와 책임 영역은 분리되어야 함 클라우드 서비스 사용에 관한 정책 및 절차를 정의해야 하며, 자신의 역할과 책임을 인식하여야 함	콘텐츠 제작팀은 기밀성이 높은 미출시 콘텐츠의 안전을 보장하며, IT 팀은 네트워크 및 시스템 보안에 중점을 둠. 클라우드 서비스 사용에 관한 정책은 각 부서에서 사용되는 클라우드 도구에 따라 세분화되며, 각 직원은 클라우드 서비스 사용 시 데이터 접근 권한 및 공유 규칙을 인식하고 준수해야 함.
연락망 (ISO/IEC27002 5.5 5.6)	조직은 관련 관계자 및 권한자와의 연락을 확립하고 유지해야 함. 조직은 특정 관심 그룹 또는 기타 전문 보안 포럼 및 전문 협회와의 연락을 확립하고 유지해야 함.	IT 보안 담당자와는 주기적인 회의 및 업데이트 세션을 통해 보안 동향 및 새로운 위협에 대한 정보를 공유함. 미디어 산업 전반에 걸친 전문 보안 포럼 및 협회와도 밀접한 연계를 유지함을 통해 업계 표준 및 모범 사례에 대한 정보를 제공받고, 새로운 보안 도구 및 기술 동향을 소개함으로써 보안 정책을 업데이트하고 강화함.
접근 권한 (ISO/IEC27002 5.15 5.18)	비즈니스 및 정보 보안 요구사항을 기반으로 정보 및 기타 관련 자산에 대한 물리적 및 논리적 접근을 제어하기 위한 규칙을 확립하고 구현해야 함. 정보 및 기타 관련 자산에 대한 접근 권한은 조직의 접근 제어에 관한 특정 주제의 정책 및 규칙에 따라 제공, 검토, 수정 및 제거되어야 함.	미디어 콘텐츠 제작팀은 미출시 콘텐츠에 대한 엑세스를 제한하고, 이에 대한 권한은 해당 부서의 담당자만이 부여받도록 함. IT 팀은 기술 시스템 및 네트워크에 대한 엑세스를 관리하며, 업무 수행에 필요한 권한만 부여받음. 접근 권한은 프로젝트 생성에 따라 정기적으로 검토되며, 변경이 필요한 경우에는 정책 및 규칙에 따라 검토, 수정, 또는 제거됨.
신원/인증 (ISO/IEC27002 5.16 5.17)	신원의 전체 수명 주기를 관리해야 함. 인증 정보의 할당 및 관리는 관리 과정에 의해 제어되어야 하며, 이에는 인증 정보의 적절한 처리에 대해 직원에게 조언하는 것도 포함되어야 함.	직원의 신원 정보는 입사 시부터 퇴사까지의 모든 단계에서 관리되며, 인증 정보의 할당 및 관리는 전체적인 관리 과정에 의해 엄격히 제어됨. 인증 정보는 해당 직무 및 업무 수행에 필요한 범위 내에서 할당되며, 이러한 할당 및 관리 과정은 IT 관리자 및 보안 팀에 의해 모니터링되며, 필요에 따라 접근 권한이 수정 또는 조정됨. 안전한 비밀번호 사용, 이메일 피싱에 대한 경각심 등에 대한 교육 및 안내 등을 통해 인증 정보의 적절한 처리에 대해 조언을 지속함.
운영 절차 (ISO/IEC27002 5.29 5.30 5.37 ISO/IEC27017 12.1.5)	조직은 중단 동안 정보 보안을 적절한 수준으로 유지하는 방법을 계획해야 함. ICT 준비는 비즈니스 연속성 목표와 ICT 연속성 요구사항을 기반으로 계획하고, 구현하고, 유지하고, 테스트되어야 함. 정보 처리 시설의 운영 절차는 문서화되어야 하며, 그것이 필요한 직원에게 제공되어야 함. 클라우드 서비스 사용자는 장애 등의 이슈로 인하여 클라우드 내 자산이 손실되어 복구가 힘들 수 있으며, 장애 처리 절차에 대하여 문서화하여야 하며 다음과 같은 내용을 포함하여야 함. - 서버, 네트워크 및 스토리지와 같은 가상화 디바이스의 설치, 변경 및 삭제 - 클라우드 서비스 사용을 위한 종료 절차 - 백업 및 복원 문서 상 작업에 대하여 모니터링하여야 함.	ICT 준비는 비즈니스 연속성 목표와 ICT 연속성 요구사항을 기반으로 계획, 구현, 유지, 주기적인 테스트를 거침. 정보 처리 시설 운영 절차는 철저하게 문서화되어 있으며, 이 문서는 해당 직원들에게 적절히 제공되도록 하여 모든 직원은 운영 절차를 명확히 이해하고 업무 수행에 필요한 지침을 얻을 수 있음. 가상화 디바이스의 설치, 변경, 삭제, 클라우드 서비스 사용 종료 절차, 그리고 백업 및 복원과 관련된 작업에 대한 모니터링을 포함한 장애 처리 절차를 상세히 문서화하여 클라우드 환경에서의 안전한 운영과 신속한 복구를 보장함.

B. 정보 관리

미디어 기업의 자산 중 컨텐츠는 단순한 지적 재산에 그치지 않는, 회사의 생명력과 같다. 컨텐츠 도난이 발생하면 제작자의 수익 창출은 물론 회사의 평판에도 중대한 영향을 미칠 수 있기에, 컨텐츠 보안의 중요성이 강조되고 있는 상황이다. 따라서 컨텐츠 관리와 더불어, 클라우드 환경상의 전반적인 정보/자산 관리 측면의 기준을 제시하고자 한다.

정보 관리 부분에 있어 주요 보안 지표는 다음과 같다.

1. 정보 관리의 통합성

- 정보 보안은 미디어 프로젝트 관리에 밀접하게 통합되어야 함.

- 미디어 및 기타 관련 자산의 목록은 소유자에 의해 개발되고 유지되어야 하며, 취급 및 사용에 대한 규칙과 절차는 식별, 문서화 되어야 함.

2. 정보 분류와 라벨링

- 정보는 기밀성, 무결성, 가용성, 그리고 이해당사자의 요구에 따라 분류되어야 함.

- 클라우드 컴퓨팅 환경에서 자산 목록은 정보 및 관련 자산의 위치를 명확히 표시하며, 클라우드 서비스 고객은 라벨링 절차를 준수하여 정보에 적절한 라벨을 부여해야 함.

3. 지식 재산권 보호

- 조직은 지식 재산권을 보호하기 위한 적절한 절차를 구현해야 함.

- 정보와 기타 관련 자산에 대한 접근은 접근 제어 정책에 따라 제한되어야 함.

4. 공급 업체와의 관리

- 공급 업체와의 관계에서 발생하는 정보 보안 위험을 관리하기 위한 프로세스와 절차를 정의하고 구현해야 함.

- 각 공급 업체와 함께 정보 보안 요구사항을 확립하고 유형에 따라 합의해야 함. 또한, ICT 제품 및 서비스 공급망과 관련된 정보 보안 위험을 관리하기 위한 프로세스를 수립하고, 공급 업체의 정보 보안 관행을 주기적으로 모니터링하고 평가해야 함.

이에 대한 세부 정책 예시는 다음과 같다.

정보 관리		
정책 조항	**이행 지침**	**정책 예시**
자산 관리 (ISO/IEC27002 5.8 5.9 5.10 5.12 5.13 8.3 ISO/IEC27017 8.1.1 8.2.2)	정보 보안은 프로젝트 관리에 통합되어야 함. 정보 및 기타 관련 자산의 목록, 포함하여 소유자는 개발되고 유지되어야 함. 정보 및 기타 관련 자산의 취급에 대한 절차와 허용 가능한 사용에 대한 규칙을 식별하고 문서화하고 구현해야 함. 정보는 기밀성, 무결성, 가용성 및 관련된 이해당사자의 요구사항을 기반으로 조직의 정보 보안 필요에 따라 분류되어야 함. 조직이 채택한 정보 분류 체계에 따라 정보 라벨링을 위한 적절한 절차 집합을 개발하고 구현해야 함. 자산 목록은 클라우드 컴퓨팅 환경에 저장된 정보 및 관련 자산을 고려해야함. 인벤토리 기록에는 자산이 유지되는 위치(예: 클라우드 서비스 식별)가 표시되어야 함. 클라우드 서비스 고객은 클라우드 서비스 고객이 채택한 라벨링 절차에 따라 클라우드 컴퓨팅 환경에서 유지 관리되는 정보 및 관련 자산에 라벨을 지정하여야 함. 정보와 기타 관련 자산에 대한 접근은 접근 제어에 관한 확립된 특정 주제의 정책에 따라 제한되어야 함.	정보 보안을 프로젝트 관리에 철저히 통합함. 모든 프로젝트는 정보 및 기타 관련 자산의 목록을 포함하며, 이 목록은 각 자산의 소유자에 의해 개발되고 유지됨. 정보 및 기타 관련 자산의 취급에 대한 절차와 허용 가능한 사용에 대한 규칙은 식별되어 문서화되고, 기업 내부의 전사적인 프로세스에 구현되어 있음. 정보는 기밀성, 무결성, 가용성 및 이해당사자의 요구사항을 기반으로 분류되며, 이를 위한 정보 분류 체계와 라벨링 절차를 개발하고 구현하고 있음. 자산 목록은 클라우드 컴퓨팅 환경에 저장된 정보 및 관련 자산을 고려하고 있으며, 클라우드 서비스 식별 및 위치 유지를 포함하여 인벤토리 기록 또한 관리됨. 기업 내 채택된 라벨링 절차에 따라 클라우드 컴퓨팅 환경에서 유지되는 정보 및 자산에 라벨을 부여하며 정보 및 기타 관련 자산에 대한 접근은 확립된 접근 제어 정책에 따라 엄격히 제한됨.
컨텐츠 관리 (ISO/IEC27002 5.12 5.32 8.3)	정보는 기밀성, 무결성, 가용성 및 관련된 이해당사자의 요구사항을 기반으로 조직의 정보 보안 필요에 따라 분류되어야 함. 조직은 지식 재산권을 보호하기 위한 적절한 절차를 구현해야 함. 정보와 기타 관련 자산에 대한 접근은 접근 제어에 관한 확립된 특정 주제의 정책에 따라 제한되어야 함.	미디어 기업의 특성에 맞춰 콘텐츠의 기밀성과 무결성을 보장하고, 가용성을 최대화하는 것을 목표로 함. 저작물에 대한 저작권은 즉각적으로 등록되고, 상표는 정기적인 감시를 통해 무단 사용을 방지함. 기술적 지식은 엄격한 접근 제어와 암호화를 통해 보호함. 라이브 스트리밍 서비스에는 암호화된 연결 및 사용자 인증을 강화하여 무단 접근을 방지하며 사용자 인증에 사용되는 개인 정보 및 결제 정보는 안전한 환경에서 처리될 수 있도록 함. 정보와 기타 관련 자산에 대한 접근은 엄격한 접근 제어 정책에 따라 제한되어 있으며, 외부 공유가 불가한 기술적 조치를 취함으로 유출 및 침해가 없도록 함.
공급망 관리 (ISO/IEC27002 5.19 5.20 5.21 5.22)	공급 업체의 제품 또는 서비스 사용과 관련된 정보 보안 위험을 관리하기 위한 프로세스와 절차를 정의하고 구현해야 함. 공급 업체 관계의 유형을 기반으로 각 공급 업체와 함께 관련 정보 보안 요구사항을 확립하고 합의해야 함. ICT 제품 및 서비스 공급망과 관련된 정보 보안 위험을 관리하기 위한 프로세스와 절차를 정의하고 구현해야 함. 조직은 공급 업체의 정보 보안 관행 및 서비스 제공에 대한 변화를 정기적으로 모니터링하고, 검토하고, 평가하고, 관리해야 함.	공급 업체 평가 및 선정 프로세스를 통해 신뢰성 있는 협력을 구축하기 위해 정보 보안 측면에서의 능력을 고려함. 공급 업체 평가 기준을 수립하고 있으며 공급 업체의 보안 정책, 기술적 대책, 그리고 이전 사례 등을 평가함.계약 및 서비스 수준 협상에서는 정보 보안 요구사항을 계약서에 명시하여 보안 수준을 명확히 확립하며, 이에는 정보 보안에 대한 책임과 규정, 보안 감사 및 모니터링 절차, 데이터 보호 등이 자세히 기술되어 있어야 함. 보안 감사 및 모니터링 측면에서는 협력 중인 공급 업체의 정보 보안 정책 및 절차를 정기적으로 감사하고, 모니터링하여 실시간으로 정보 보안 수준을 평가함. 위기 대응 및 대비에 대해서는 긴급한 상황에 대비하여 협력 관계에서의 위기 대응 및 대비 계획을 수립하며, 지속적인 교육과 국제 정보보안 인증 취득 등을 요구해야 함.

C. 사고 관리

최근, 유명 미디어 및 엔터테인먼트 회사에 대한 해킹이 발생하여 데이터 손실 및 생산성과 운영에 타격이 발생하였으며, 정보 유출로 이어지기까지 한 사례가 있었다. 초기 보안 이벤트 탐지에 실패해 연쇄적인 침해가 발생했으며, 상당한 기업 이미지 타격을 입기도 했다. 이와 같은 보안 사고를 방지하기 위해 침해사고 대응 전략과 위협 인텔리전스 축적에 따른 고도화 프로세스 등, 사고 관리 전반에 걸친 보안 기준을 제시하고자 한다.

사고 관리 부분에 있어 주요 보안 지표는 다음과 같다.

1. 위협 인텔리전스 및 정보 수집

- 조직은 정보 보안 위협과 관련된 정보를 수집하고 분석하여 위협 인텔리전스를 생성해야 함.

2. 정보 보안 사고 관리 계획과 프로세스

- 조직은 정보 보안 사고 관리 프로세스, 역할, 책임을 정의하고 확립하여 정보 보안 사고에 대한 계획과 대비를 수립해야 함.

3. 정보 보안 이벤트 평가 및 응답

- 조직은 정보 보안 이벤트를 평가하고 사고로 분류할지 결정한 후, 문서화된 절차에 따라 신속하게 응답해야 함.

4. 사고로부터 얻은 지식을 활용

- 정보 보안 사고에서 얻은 지식은 조직이 정보 보안 제어를 강화하고 개선하는 데 사용되어야 함.

5. 증거 관리 및 보존

- 조직은 정보 보안 이벤트와 관련된 증거의 식별, 수집, 획득, 보존을 위한 절차를 확립하고 구현하여 기록을 보호해야 함.

6. 클라우드 서비스 고객과의 협력

- 클라우드 서비스 고객은 정보 보안 사고 관리를 위한 책임 할당을 확인하고, 클라우드 서비스 공급자에게 필요한 정보를 정기적으로 요청하여야 함. 또한, 사고 관리에 대한 상호 협력 및 정보 교환을 위한 메커니즘을 마련해야 함.

이에 대한 세부 정책 예시는 다음과 같다.

사고 관리		
정책 조항	**이행 지침**	**정책 예시**
침해사고 대응 절차 (ISO/IEC27002 5.7 5.24 5.25 5.26 5.27 5.28 5.33)	정보 보안 위협과 관련된 정보는 수집되고 분석되어 위협 인텔리전스를 생성해야 함. 조직은 정보 보안 사고 관리 프로세스, 역할 및 책임을 정의하고, 확립하고, 의사소통함으로써 정보 보안 사고를 관리하기 위한 계획과 준비를 해야 함. 조직은 정보 보안 이벤트를 평가하고, 그것들이 정보 보안 사고로 분류될 것인지 결정해야 함. 문서화된 절차에 따라 정보 보안 사고에 응답해야 함. 정보 보안 사고에서 얻은 지식은 정보 보안 제어를 강화하고 개선하는 데 사용되어야 함. 조직은 정보 보안 이벤트와 관련된 증거의 식별, 수집, 획득 및 보존을 위한 절차를 확립하고 구현해야 함. 기록은 손실, 파괴, 조작, 무단 접근 및 무단 공개로부터 보호되어야 함.	미디어 산업에서의 정보 보안 위협에 대비하기 위해 다음과 같은 구체적인 절차와 정책을 시행함. 실시간 위협 분석: 미디어 기업의 특성을 고려하여 실시간으로 발생하는 정보 보안 위협을 모니터링하고 분석함. 이를 통해 즉각적으로 대응할 수 있는 인텔리전스를 확보함. 정보 보안 사고 대응 계획: 사고 발생 시를 대비하여 명확한 대응 계획을 수립함. 역할 및 책임을 명확히하고 의사소통을 원활히 하여 효과적인 대응을 할 수 있도록 함. 이벤트 평가 및 분류: 발생한 정보 보안 이벤트를 신속하게 평가하고 그것이 사고로 분류될지를 결정하는 명확한 절차를 운영함. 절차에 따른 신속한 대응: 문서화된 절차에 따라 사고에 신속하게 대응하여 추가 피해를 최소화하고, 발생한 이벤트를 통해 얻은 지식을 활용하여 제어를 강화하고 개선함. 증거 보존 및 분석: 사고 조사를 위한 명확한 증거 보존 및 분석 절차를 운영하여 효과적인 조사를 진행함. 이를 통해 사고로부터의 교훈을 얻고 제어 강화에 활용함. 지속적인 향상: 발생한 이벤트를 토대로 지속적으로 보안 제어를 향상시키고, 새로운 위협에 대비하기 위한 계획을 수립함. 이를 통해 정보 보안 수준을 지속적으로 향상시킴.
침해사고 대응에 있어 CSP 의 역할 (ISO/IEC27017 16.1.1 16.1.2 16.1.7)	정보 보안 사고 관리를위한 책임 할당을 확인하고 클라우드 서비스 고객의 요구 사항을 충족하는지 확인하여야 함. 클라우드 서비스 고객은 클라우드 서비스 공급자에게 다음과 같은 메커니즘에 대한 정보를 요청하여야 함. - 클라우드 서비스 고객이 감지한 정보 보안 이벤트를 클라우드 서비스 공급자에게 보고 - 클라우드 서비스 공급자가 클라우드 서비스 공급자가 탐지한 정보 보안 이벤트와 관련된 보고서 수신 - 클라우드 서비스 고객이보고된 정보 보안 이벤트의 상태를 추적 클라우드 서비스 사용자 및 제공자는 잠재적인 디지털 증거 또는 클라우드 환경에서의 기타 요청에 대한 회신 절차에 동의 하여야 함.	클라우드 서비스 활용에 대한 침해사고 대응에 있어, 명확한 책임 할당을 정의하기 위해 다음과 같은 메커니즘을 시행함. 책임 할당 확인: 정보 보안 사고 발생 시 각 담당자에게 명확한 책임과 역할을 부여하여 신속하고 효과적인 대응이 이루어질 수 있도록 함. 클라우드 서비스 요구사항 확인: 감지한 정보 보안 이벤트를 즉시 클라우드 서비스 공급자에게 보고하는 절차를 마련함. CSP 로부터 탐지된 이벤트와 관련된 보고서를 효율적으로 수신함. 이벤트 상태 추적: CSP 로부터 보고된 정보 보안 이벤트의 상태를 추적하고, CSP 와의 소통을 통해 사건의 진행 상황을 정확히 파악함. 디지털 증거 회신 절차 동의: 자사 및 CSP 는 잠재적인 디지털 증거 또는 클라우드 환경에서의 기타 요청에 대한 회신 절차에 동의하고, 이를 통해 즉각적이고 투명한 협력을 유지함.

3. 인적 보안

본 인적 보안 목차는 미디어 기업의 인적 자원 고용 전/중/후에 걸쳐 고려해야 할 보안상 주안점을 정리하고 있다. 고용 전 지원자 정보에 대한 스크리닝, 고용 중 고용자 대상의 정보보호 서약 및 필수 이수의 보안 교육 내용, 고용 후 권한 반환에 대한 내용을 포함하고 있다. 이를 통해 조직은 항상 보안상 최대 취약점으로 언급되는 인적 자원에 대한 보안 우려를 줄여나갈 수 있다.

인적 보안 부분에 있어 주요 보안 지표는 다음과 같다.

1. 인사 전 및 후 배경 검증

- 인사 후보의 정보 보안 적합성을 확인하기 위해 조직은 법률, 규정, 윤리, 비즈니스 요구사항 및 정보의 분류에 따라 배경 검증을 수행해야 함.

- 고용 계약 합의는 직원과 조직의 정보 보안 책임을 명시해야 함.

2. 정보 보안 인식과 교육

- 직원 및 이해당사자들은 정보 보안 정책 및 절차에 대한 업데이트를 정기적으로 받아야 함.

- 정보 보안 정책을 위반한 경우에 대한 징계 절차를 공식화하고 전달해야 함.

- 기밀성 또는 누설 금지 합의는 확인, 문서화, 검토, 서명되어야 하며 정기적으로 갱신되어야 함.

3. 원격 작업 환경에서의 정보 보안

- 원격 작업 시, 정보에 접근, 처리, 저장을 보호하기 위한 보안 조치가 시행되어야 함.

- 직원은 관찰 또는 의심되는 정보 보안 사건을 신속하게 보고할 수 있는 메커니즘을 제공해야 함.

4. 클라우드 서비스 사용자 교육

- 클라우드 서비스와 관련된 표준, 절차, 정보 보안 위험 및 관리 방법에 대한 교육이 필요함.

- 적용 가능한 법적 및 규제 사항에 대한 교육이 제공되어야 함.

5. 고용 및 계약 종료

- 직원 및 관련 이해당사자는 고용 종료 시, 조직 자산을 반환해야 함.

- 고용 종료나 직무 변경 후에도 정보 보안 의무가 유효하게 유지되어야 하며, 관련 당사자에게 알려져야 함.

이에 대한 세부 정책 예시는 다음과 같다.

인적 보안		
정책 조항	**이행 지침**	**정책 예시**
고용 전 (ISO/IEC27002 6.1 6.2)	조직에 합류하기 전 및 지속적으로 모든 인사 후보에 대한 배경 검증 확인이 진행되어야 함. 적용 가능한 법률, 규정, 윤리를 고려하며, 비즈니스 요구사항, 접근될 정보의 분류 및 인식된 위험에 비례하여 이루어져야 함. 고용 계약 합의는 직원과 조직의 정보 보안에 대한 책임을 명시해야 함.	채용 전 및 모든 인사 후보에 대해 철저한 배경 검증을 수행함. 이 프로세스는 적용 가능한 법률, 규정, 윤리를 엄격히 준수하며, 우리 비즈니스 요구사항과 정보의 분류, 그리고 인식된 위험 수준에 따라 조절됨. 모든 고용 계약에서 직원과 우리 조직 간의 정보 보안에 대한 책임을 명확히 기술함. 이를 통해 우리는 직원들이 정보 자산을 적절히 처리하고 보호하는 데 필요한 책임을 이해하고 준수할 수 있음.
고용 중 (ISO/IEC27002 6.36.4 6.6 6.7 6.8 ISO/IEC27017 7.2.2)	조직의 직원 및 관련 이해당사자들은 그들의 직무 기능에 관련된 조직의 정보 보안 정책, 특정 주제에 관한 정책 및 절차의 정기적인 업데이트와 함께 적절한 정보 보안 인식, 교육 및 교육을 받아야 함. 정보 보안 정책을 위반한 직원 및 기타 관련 이해당사자에 대한 조치를 취하기 위해 징계 절차를 공식화하고 전달해야 함. 정보 보호를 위한 조직의 요구를 반영하는 기밀성 또는 누설 금지 합의는 확인되고, 문서화되며, 정기적으로 검토되고, 직원 및 기타 관련 이해당사자들에 의해 서명되어야 함. 직원들이 원격으로 작업할 때 조직의 장소 외부에서 접근, 처리 또는 저장된 정보를 보호하기 위해 보안 조치를 시행해야 함. 조직은 직원들이 관찰하거나 의심되는 정보 보안 사건을 적절한 채널을 통해 신속하게 보고할 수 있는 메커니즘을 제공해야 함. 클라우드 서비스 비즈니스 관리자, 클라우드 서비스 관리자, 클라우드 서비스 통합 자 및 클라우드 서비스 사용자(관련 직원 및 계약자 포함)에 대한 인식, 교육 및 교육 프로그램에 다음 항목을 추가하여야 함. - 클라우드 서비스 사용을위한 표준 및 절차 - 클라우드 서비스와 관련된 정보 보안 위험 및 이러한 위험 관리 방법 - 클라우드 서비스의 사용으로 인한 시스템 및 네트워크 환경 위험 - 적용 가능한 법적 및 규제 사항	직원 및 관련 이해당사자들이 자신의 직무와 관련된 정보 보안 정책 및 절차에 대한 최신 정보를 정기적으로 받을 수 있도록 전용 소통창을 개설함. 정보 보안 정책을 위반한 경우에는 직원 및 관련 이해당사자에 대한 징계 절차를 명확하게 공식화하고 전달하여 신속하게 대응하며, 밀성 또는 누설 금지 합의를 문서화하고 정기적으로 검토하여 직원 및 이해당사자들이 요구사항을 이해하고 준수하도록 함. 원격 근무 시에는 외부에서의 정보 접근을 효과적으로 제어하기 위해 VPN, MFA, 원격 데스크톱 서비스를 의무적으로 사용하도록 함. 직원들이 관찰하거나 의심되는 정보 보안 사건을 신속하게 보고할 수 있도록 메커니즘을 제공함. 클라우드 서비스와 관련된 직원 및 계약자에 대한 인식, 교육 및 교육 프로그램에는 클라우드 서비스 사용을위한 표준 및 절차, 정보 보안 위험 및 관리 방법, 시스템 및 네트워크 환경 위험, 그리고 적용 가능한 법적 및 규제 사항에 대한 교육을 반기별로 시행함.
고용 후 (ISO/IEC27002 5.11 6.5)	직원 및 적절한 경우 다른 관심 당사자는 고용, 계약 또는 합의의 변경 또는 종료시 그들이 보유하고 있는 조직의 모든 자산을 반환해야 함. 고용 종료나 직무 변경 후에도 유효한 정보 보안 책임과 의무를 정의하고, 시행하며, 관련 직원 및 기타 관심 당사자들에게 알려야 함.	직원 및 필요한 경우 다른 이해당사자는 고용, 계약 또는 합의의 변경 또는 종료 시 조직의 모든 자산을 즉시 반환해야 함. 고용 종료 또는 직무 변경 이후에도 유효한 정보 보안 책임과 의무를 명확하게 정의하고 시행하며, 관련 직원 및 기타 이해당사자들에게 명확하게 알림.

4. 물리 보안

본 물리 보안 목차는 미디어 기업의 물리 보안 전반의 관리 방안, 주요 접근 통제 방안, 운영에 있어 물리 보안 주안점을 정리하고 있다. 물리 보안 설계를 위한 기본적인 전략 설계와 물리 보안의 기본이 되는 접근 통제 방법론, 세세한 물리 보안 운영 방안에 대한 내용을 포함하고 있다. 이를 통해 조직은 물리 보안의 초석을 마련하고, 자체적인 물리 보안 문화를 형성해 나갈 수 있다.

물리 보안 부분에 있어 주요 보안 지표는 다음과 같다.

1. 보안 퍼리미터의 정의와 활용

- 정보와 기타 관련 자산이 포함된 영역을 보호하기 위해 명확한 보안 퍼리미터를 정의하고 사용해야 함.

- 자연 재해 및 의도적, 우발적인 물리적 및 환경적 위협에 대비하여 설계된 보호 조치를 구현해야 함.

2. 안전한 영역에서의 작업 보안 조치

- 안전한 영역에서의 작업을 위한 보안 조치는 설계되고 구현되어야 함.

- 장비는 안전하게 위치시키고 보호되어야 하며, 외부 자산 또한 신중하게 보호되어야 함.

3. 출입 통제 및 물리적 보안

- 안전한 영역은 출입 통제 및 적절한 접근 지점에 의해 보호되어야 함.

- 사무실, 방, 및 시설에 대한 물리적 보안은 설계되고 구현되어야 하며, 무단 물리적 접근은 지속적으로 모니터링되어야 함.

4. 저장 매체 및 정보 처리 시설 관리

- 서류 및 이동식 저장 매체에 대한 책상 정리 규칙 및 정보 처리 시설에 대한 깨끗한 화면 규칙이 정의되고 시행되어야 함.

- 저장 매체는 조직의 분류 체계와 처리 요구 사항에 따라 획득, 사용, 운송, 및 폐기의 수명 주기 동안 관리되어야 함.

5. 전력, 데이터, 및 케이블 보안

- 정보 처리 시설은 전원 장애 및 지원 공공 시설의 장애로부터 보호되어야 함.

- 전력, 데이터, 또는 지원 정보 서비스를 운반하는 케이블은 가로채기, 간섭, 또는 손상으로부터 보호되어야 함.

6. 유지보수 및 폐기 전 검증

- 정보의 가용성, 무결성, 및 기밀성을 보장하기 위해 장비는 올바르게 유지보수되어야 하며, 폐기 전에는 민감한 데이터와 라이선스된 소프트웨어가 안전하게 제거 또는 덮어쓰였는지 확인되어야 함.

이에 대한 세부 정책 예시는 다음과 같다.

물리 보안		
정책 조항	**이행 지침**	**정책 예시**
물리 보안 관리 (ISO/IEC27002 7.1 7.5 7.6 7.8 7.9 ISO/IEC 27017 11.2.7)	정보와 기타 관련 자산이 포함된 영역을 보호하기 위해 보안 퍼리미터를 정의하고 사용해야 함. 자연 재해 및 인프라에 대한 의도적 또는 우발적인 물리적 위협과 같은 물리적 및 환경적 위협에 대한 보호는 설계되고 구현되어야 함. 안전한 영역에서의 작업을 위한 보안 조치는 설계되고 구현되어야 함. 장비는 안전하게 위치시키고 보호해야 함 외부 자산은 보호되어야 함 클라우드 서비스 고객은 클라우드 서비스 공급자가 리소스의 안전한 폐기 또는 재사용을 위한 정책과 절차를 가지고 있다는확인을 요청하여야 함.	정보와 자산을 보호하기 위해 건물 내 및 주변에 명확한 보안 경계를 설정하고 CCTV 와 출입 제어 시스템을 운영함. 자연재해에 대비하여 서버 및 중요한 장비는 빅데이터 기반 추천 지역을 선별하여 분산하여 위치함. 클라우드 서비스 공급자가 리소스를 안전하게 폐기하거나 재사용하기 위한 정책과 절차를 갖추고 있는지 지속적으로 확인하며, 변동 사항에 대한 보고 프로세스를 확립함.
접근 통제 (ISO/IEC27002 7.2 7.3 7.4)	안전한 영역은 적절한 출입 통제 및 접근 지점에 의해 보호되어야 함. 사무실, 방 및 시설에 대한 물리적 보안은 설계되고 구현되어야 함. 무단 물리적 접근을 지속적으로 모니터링해야 함.	사무실, 각 방, 그리고 기타 시설에 대한 출입은 승인된 직원들만이 가능하도록 생체정보 기반 출입 시스템을 도입함. CCTV 카메라, 보안 경비원, 그리고 출입 기록 등을 통해 물리적 보안을 제고하며, 방문자 및 외부인에 대한 출입은 방문 예약, 사전 정보 제출, 사전 승인 및 검토, 방문 시 규정 준수라는 확립된 프로세스에 의해 관리됨. 무단 물리적 접근에 대한 방지를 위해 모니터링 시스템을 운영하며, 출입 기록 및 CCTV 영상을 정기적으로 검토하여 이상 행동이나 무단 출입을 감지하고 조치를 취함.
운영 (ISO/IEC27002 7.7 7.10 7.11 7.12 7.13 7.14)	서류 및 이동식 저장 매체에 대한 깨끗한 책상 규칙과 정보 처리 시설에 대한 깨끗한 화면 규칙은 정의되어야 하며 적절하게 시행되어야 함. 저장 매체는 조직의 분류 체계와 처리 요구 사항에 따라 획득, 사용, 운송 및 폐기의 수명 주기 동안 관리되어야 함. 정보 처리 시설은 전원 장애 및 지원 공공 시설의 장애로 인한 다른 중단으로부터 보호되어야 함 전력, 데이터 또는 지원 정보 서비스를 운반하는 케이블은 가로채기, 간섭 또는 손상으로부터 보호되어야 함. 정보의 가용성, 무결성 및 기밀성을 보장하기 위해 장비는 올바르게 유지보수되어야 함. 저장 매체를 포함하는 장비 항목은 처분 또는 재사용 전에 민감한 데이터와 라이선스된 소프트웨어가 제거되거나 안전하게 덮어쓰였는지 확인되어야 함.	모든 직원 및 이해당사자는 정보 보안을 위해 제시된 청결 규칙을 준수해야 하며, 저장 매체는 분류 체계와 처리 요구 사항에 따라 관리되어야 함. 케이블의 안전한 배치 규칙을 준수하고, 분기별 정기 장비 점검을 진행해야 하며 처분 시엔 민감 정보에 대한 완전한 삭제 조치가 취해져야 함. 청결규칙: 1.모든 서류 및 저장 매체는 정해진 보안 정책에 따라 적절하게 분류되고 관리되어야 함 2.정보 처리 시설은 주기적인 청소 프로토콜에 따라 유지되어야 하며, 화면은 민감한 정보가 노출되지 않도록 깨끗이 유지하며, 작업 영역은 비사용 시 잠금이 되어야 함. 케이블 배치 규칙: 1.케이블 보호 및 경로 지정: 물리적 손상으로부터 보호하기 위해 보호커버나 특수한 채널을 활용함.

		2.라벨링 및 식별: 케이블이 어떤 기기 또는 시스템과 연결되어 있는지 식별하도록 함. 3.배치 및 안전한 공간: 케이블은 정돈되고 청결하게 배치되어야 하며, 걸리거나 밟히지 않도록 안전한 위치에 배치되어야 함.

5. 기술적 보안

본 기술적 보안 목차는 미디어 기업의 정보보호 전략 전반에 있어 활용되어야 할 기술 보안 조치 내용을 정리하고 있다. 기술적 차원에서의 권한 관리 방안과 데이터 관리 방안, 소프트웨어 개발 및 프로젝트 진행 시 발생할 수 있는 보안 취약점과 점검 항목을 포함하고 있다. 인프라에 대한 기술적 보안 조치, 암호화 기준과 활용 분야, 백업/로깅/모니터링 전반에 대한 관리상 주안점과 응용 프로그램 사용에 대한 보안 고려점을 포함하고 있다. 이를 통해 조직은 미디어 산업의 특징과 클라우드 사용에 대한 요구사항을 충족시키는 기술적 보안 조치를 취할 수 있다.

기술적 보안 부분에 있어 주요 보안 지표는 다음과 같다.

1. 특권 액세스와 정보 접근 제어

- 특권 액세스 권한은 제한되고 감독되어야 함.

- 정보와 기타 자산에 대한 접근은 접근 제어 정책을 기반으로 제한되며, 소스 코드 및 개발 도구에 대한 권한은 적절하게 관리되어야 함.

2. 클라우드 서비스 고객의 네트워크 서비스 액세스

- 클라우드 서비스 고객은 네트워크 서비스 사용에 대한 액세스 제어 정책을 정의하여야 함.

- 클라우드 서비스 관리자는 확인된 위험에 따라 충분한 인증 기술을 사용하여 클라우드 서비스의 관리 기능을 보호해야 함.

3. 데이터 보안과 관련된 주요 규칙

- 사용자 엔드포인트 장치를 통해 저장된 정보는 보호되어야 하며, 민감한 정보는 데이터 마스킹을 통해 안전하게 처리되어야 함.

- 데이터 누출 방지 조치는 시스템, 네트워크, 및 기타 장치에 적용되어야 함.

4. 소프트웨어 및 시스템의 안전한 개발과 관련된 정책

- 소프트웨어 개발 시 안전한 코딩 원칙을 적용하고, 보안 테스트 프로세스를 개발 수명 주기에 통합해야 함.

- 시스템 엔지니어링 원칙은 안전한 설정, 문서화, 유지, 및 개발 활동에 적용되어야 함.

5. 취약성 관리 및 보안 테스트

- 시스템의 기술적 취약성에 대한 정보를 획득하고, 외부 시스템 개발과 관련된 활동을 모니터링하며, 보안 테스트 프로세스를 개발 수명 주기에 통합해야 함.

- 클라우드 서비스 사용자는 제공된 클라우드 서비스에 영향을 줄 수 있는 기술적 취약성 관리를 클라우드 서비스 공급자에게 요청해야 함.

6. 암호화 및 보안키 관리

- 암호화의 효과적인 사용을 위한 정책과 암호화 키 관리가 정의되고 구현되어야 함.

- 클라우드 서비스 고객은 클라우드 서비스 공급자가 제공한 정보의 암호화 적절성을 확인하고, 자체 키 관리를 사용할 경우 관리 절차를 명확하게 정의해야 함.

7. 자원의 사용 및 이벤트 모니터링

- 자원의 사용은 현재와 예상되는 용량 요구 사항과 일치하도록 모니터링되고 조정되어야 함.

- 활동, 예외, 결함, 및 이벤트를 기록하고 분석하기 위한 로그는 적절하게 생성되고 보호되어야 함.

8. 기술적 보안과 관련된 제어 조치

- 유틸리티 프로그램의 사용은 엄격하게 통제되어야 하며, 운영 시스템에 소프트웨어 설치는 안전한 절차와 조치를 통해 관리되어야 함.

- 클라우드 서비스 사용자는 라이센스가 부여된 소프트웨어를 클라우드 서비스에 설치하기 전에 관련 라이센스 요구사항을 확인하는 절차를 갖추어야 함.

이에 대한 세부 정책 예시는 다음과 같다.

기술적 보안		
정책 조항	**이행 지침**	**정책 예시**
권한 관리 (ISO/IEC27002 8.2 8.3 8.4 8.5 ISO/IEC27017 9.1.2 9.2.3 9.2.4 9.4.1 12.4.3)	특권 액세스 권한의 할당과 사용은 제한되고 관리되어야 함. 정보와 기타 관련 자산에 대한 접근은 접근 제어에 관한 확립된 특정 주제의 정책에 따라 제한되어야 함. 소스 코드, 개발 도구 및 소프트웨어 라이브러리에 대한 읽기 및 쓰기 권한은 적절하게 관리되어야 함.	소스 코드, 개발 도구, 그리고 소프트웨어 라이브러리 등과 관련된 특별한 액세스 권한을 필요한 직무에 한정하여 부여하며, 수행하는 업무에 필요한 권한만만을 허용하고 불필요한 권한 제한, 프로젝트 변동에 따른 최소 권한 허용 원칙 등을 바탕으로 엄격한 접근 제어 정책을 실시함.

	정보 접근 제한과 접근 제어에 관한 특정 주제의 정책을 기반으로 안전한 인증 기술과 절차를 구현해야 함. 클라우드 서비스 고객의 네트워크 서비스 사용에 대한 액세스 제어 정책은 사용되는 각 클라우드 서비스에 대한 사용자 액세스 요구 사항을 지정하여야 함. 확인 된 위험에 따라 클라우드 서비스 고객의 클라우드 서비스 관리자가 클라우드 서비스의 관리 기능을 인증 할 수 있도록 충분한 인증 기술(예: 다중 요소 인증)을 사용하여야 함. 클라우드 서비스 고객은 클라우드 서비스 공급자의 암호와 같은 비밀 인증 정보를 할당하는 관리 절차가 클라우드 서비스 고객의 요구 사항을 충족하는지 확인하여야 함. 클라우드 서비스의 정보에 대한 액세스가 액세스 제어 정책에 따라 제한되고 이러한 제한이 실현되는지 확인하여야 함. 여기에는 클라우드 서비스, 클라우드 서비스 기능 및 서비스에서 유지 관리되는 클라우드 서비스 고객 데이터에 대한 액세스 제한이 포함된다.	대/소문자, 숫자 및 특수문자 조합과 같은 강력한 암호 사용을 의무화 하고있으며, 중요한 시스템이나 기밀 정보에 접근할 때는 추가적인 인증 단계를 적용시켜 안전한 인증 절차가 가능하도록 함. 클라우드 서비스 상에서 정보에 접근할 때 또한 안전한 신원 확인을 위해 다단계 인증 및 생체 인식과 같은 첨단 보안 기술을 활용하며, 사용자가 필요로 하는 서비스에만 접근하고 필요한 최소한의 정보만이 노출되도록 기술적 설계를 진행함.
데이터 관리 (ISO/IEC27002 8.1 8.10 8.11 8.12)	사용자 엔드포인트 장치를 통해 저장된, 처리된 또는 접근 가능한 정보는 보호되어야 함. 정보 시스템, 장치 또는 다른 저장 매체에 저장된 정보는 더 이상 필요하지 않을 때 삭제되어야 함. 데이터 마스킹은 조직의 접근 제어 및 다른 관련 주제의 정책, 비즈니스 요구 사항 및 적용 가능한 법률을 고려하여 사용되어야 함. 민감한 정보를 처리, 저장 또는 전송하는 시스템, 네트워크 및 기타 장치에 데이터 누출 방지 조치를 적용해야 함.	사용자 엔드포인트 장치를 통한 정보 처리 및 저장에 대한 안전한 보호를 위해 모든 엔드포인트 장치는 최신의 보안 소프트웨어 및 업데이트를 진행하도록 하며, 기업 공동의 보안 도구가 활성화 되어있도록 함. 모든 정보 시스템, 장치, 그리고 다른 저장 매체에 저장된 정보는 불필요해지면 덮어쓰기의 방식으로 완전 삭제되며 민감한 정보를 처리, 저장, 또는 전송하는 시스템, 네트워크, 그리고 다른 장치에는 데이터 누출 방지를 위해 데이터 마스킹 및 암호화 기술을 활용함.
개발 보안 (ISO/IEC27002 8.25 8.26 8.27 8.28 8.29 8.30 8.31 8.33 ISO/IEC27017 14.2.1)	소프트웨어 및 시스템의 안전한 개발을 위한 규칙이 수립되고 적용되어야 함. 응용 프로그램을 개발하거나 획득할 때 정보 보안 요구 사항을 식별, 명시 및 승인해야 함. 안전한 시스템 엔지니어링 원칙은 설정, 문서화, 유지 및 모든 정보 시스템 개발 활동에 적용되어야 함. 소프트웨어 개발에 안전한 코딩 원칙이 적용되어야 함. 보안 테스트 프로세스는 개발 수명 주기에 정의되고 구현되어야 함. 조직은 외부 시스템 개발과 관련된 활동을 지시하고 모니터링하며 검토해야 함. 개발, 테스트 및 운영 환경은 분리되어야 하며 보호되어야 함. 테스트 정보는 적절하게 선택되어 보호되고 관리되어야 함.	새로운 응용 프로그램을 개발하거나 도입할 때에는 해당 프로젝트의 정보 보안 요구 사항을 명확하게 식별하고 명시하며, 이에 필요한 승인 프로세스를 문서화하여 확실히 진행될 수 있도록 함. 안전한 시스템 엔지니어링 원칙은 모든 정보 시스템 개발 단계에서 적용되어 안전한 코딩 원칙을 준수하며, 보안 테스트 프로세스를 개발 수명 주기에 통합하여 안정적인 시스템을 구축함. 외부 시스템 개발과 관련된 활동은 조직 내에서 명확한 지시를 받아 진행되고, 그 과정에서 안전성을 지속적으로 검토하고 강화함. 개발, 테스트, 그리고 운영 환경은 분리되어 운영되며, 테스트 정보는 신중히 선택되어 보호되고 관리되어 안전한 개발 환경을 유지함.
인프라 보안 (ISO/IEC27002 8.7 8.8 8.9 8.14 8.20 8.21 8.22 8.23 8.32 8.34 ISO/IEC27017 12.6.1 13.1.3 9.5.2)	악성 소프트웨어에 대한 보호는 적절한 사용자 인식을 지원하고 구현되어야 함. 사용 중인 정보 시스템의 기술적 취약점에 관한 정보를 획득하고, 조직의 해당 취약성에 대한 노출을 평가하고, 적절한 조치를 취해야 함. 하드웨어, 소프트웨어, 서비스 및 네트워크의 구성(보안 구성 포함)은 확립, 문서화, 구현, 모니터링 및 검토되어야 함. 정보 처리 시설은 가용성 요구 사항을 충족시키기에 충분한 중복성을 갖추어 구현되어야 함. 네트워크 및 네트워크 장치는 시스템 및 애플리케이션의 정보를 보호하기 위해 안전하게 관리되고 제어되어야 함.	하드웨어, 소프트웨어, 서비스, 및 네트워크의 구성은 철저하게 확립되어 문서화되고, 구현되며, 지속적으로 모니터링과 검토를 진행함. 정보 처리 시설은 가용성 요구 사항을 충족시키기 위해 설계되었으며, 라이브 스트리밍 서비스는 Auto Scailing 그룹에 속하고 컨텐츠 저장 서버는 분산되어 위치하며, 각 데이터 센터마다 이중화 이상의 배치를 의무화함. 네트워크 서비스의 보안 메커니즘, 서비스 수준, 및 서비스 요구 사항은 식별되어 구현되며 지속적으로 모니터링되어 정보 보안을 강화함. 내부의 정보 서비스, 사용자, 및 정보 시스템의 그룹은 효과적으로 분리되어

	네트워크 서비스의 보안 메커니즘, 서비스 수준 및 서비스 요구 사항은 식별되고 구현되며 모니터링되어야 함. 조직의 네트워크에서 정보 서비스, 사용자 및 정보 시스템의 그룹은 분리되어야 함. 외부 웹사이트 접근은 악성 콘텐츠에 노출을 줄이기 위해 관리되어야 함. 정보 처리 시설 및 정보 시스템의 변경은 변경 관리 절차에 따라 이루어져야 함. 운영 시스템 평가를 포함하는 감사 테스트 및 기타 확인 활동은 테스터와 적절한 관리 간에 계획되고 합의되어야 함. 제공된 클라우드 서비스에 영향을 줄 수있는 기술적 취약성 관리에 관해 클라우드 서비스 공급자에게 정보를 요청하여야 함. 클라우드 서비스 고객은 관리해야 할 기술적 인 취약점을 파악하고 이를 관리하는 프로세스를 명확하게 정의하여야 함. 클라우드 서비스의 공유 환경에서 테넌트 격리를 달성하고 클라우드 서비스 공급자가 이러한 요구 사항을 충족하는지 확인하기 위해 네트워크 분리에 대한 요구 사항을 정의하여야 함. 가상 머신을 구성하는 경우, 클라우드 서비스 사용자 및 제공자는 적절한 기술적 조치 및 보안환경 설정을 확인하여야 함. - 불필요 포트 및 프로토콜, 서비스 제거 - 악성코드 방지 및 로깅	있으며, 외부 웹사이트 접근은 악성 콘텐츠에 노출을 최소화하기 위해 화이트리스트 기반으로 접근을 허용하며 필요 시 별도 분리망을 이용하도록 함. 사용 중인 정보 시스템의 기술적 취약점에 대한 정보를 정기적으로 확인하며, 이를 평가하여 조직의 취약성을 신속히 파악하고, 필요한 보안 조치를 실시함. 정보 처리 시설 및 정보 시스템의 변경은 요청 및 식별, 평가 및 승인, 계획, 테스트, 도입 및 적용, 문서화, 평가 및 모니터링의 철저한 절차에 한해 이뤄지며, 클라우드 서비스 상의 자산 변경은 최소한의 트래픽을 허용되도록 설계되며 이후 보고 및 승인의 절차에 따라 확장되는 메커니즘을 구현함. 운영 시스템 평가를 포함하는 감사 테스트 또한 외부의 감사인에 의해 회계년도마다 시행함. 가상 머신의 경우 불필요한 포트 및 프로토콜, 서비스를 제거하고, 악성코드 방지 및 로깅을 통한 보안환경 설정을 확인하여 안전한 가상 환경을 확보하며, CSP 에게 영향을 줄 수 있는 기술적 취약성에 대한 정보를 요청하여 관리함. 라우드 서비스의 공유 환경에서 테넌트 격리를 달성하고 네트워크 분리를 위한 요구 사항을 정의하여 시스템의 보안성을 지속적으로 강화함.
암호화 (ISO/IEC27002 8.24 ISO/IEC27017 10.1.1 10.1.2)	암호화의 효과적인 사용을 위한 규칙, 암호화 키 관리를 포함한 것이 정의되고 구현되어야 함. 클라우드 서비스 공급자가 암호화를 제공하면 클라우드 서비스 고객은 클라우드 서비스 공급자가 제공 한 모든 정보를 검토하여 암호화 적절한지 확인하여야 함. 클라우드 서비스 고객은 자체 클라우드 서비스 고객이 자체 키 관리 또는 별개의 키 관리 서비스를 사용하는 경우 클라우드 서비스 공급자가 암호화 작업을 위한 암호화 키를 저장하고 관리하도록 허용하여서는 안된다.	최소한 AES-256 과 같은 강력한 대칭키 알고리즘을 사용하여 민감한 정보의 암호화를 진행하며, 공개키 알고리즘을 통해 안전한 키 교환을 지원힘. 암호화 키 관리에 있어 키는 별도의 망에 이중 암호화 되어 보관되며, 액세스 권한은 필수적인 인증 및 권한 확인 절차를 거쳐 제한되고 주기적인 회전 및 업데이트는 회사 내부 보안 프로그램에 의해 자동적으로 수행됨. 클라우드 서비스 내의 키 관리를 자체 키 관리 방식으로 수행하며, 키에 대한 최소 접근 권한 할당과, 키 접근 로깅을 철저히 진행함. 키 분배는 원칙상 금지되며, 권한 할당으로 대체할 수 있는 경우 추가 권한 할당 부문을 분석하여 진행함.
백업/로깅/모니터링 (ISO/IEC27002 8.6 8.13 8.15 8.16 8.17 ISO/IEC27017 12.3.1 12.4.1 12.4.5)	자원의 사용은 현재 및 예상되는 용량 요구 사항과 일치하도록 모니터링되고 조정되어야 함. 정보, 소프트웨어 및 시스템의 백업 사본은 합의된 백업 주제의 정책에 따라 유지되고 정기적으로 테스트되어야 함. 활동, 예외, 결함 및 기타 관련 이벤트를 기록하는 로그는 생성되고 저장되며 보호되고 분석되어야 함. 네트워크, 시스템 및 애플리케이션은 비정상적인 동작을 모니터링하고, 잠재적인 정보 보안 사건을 평가하기 위한 적절한 조치를 취해야 함. 조직이 사용하는 정보 처리 시스템의 시계는 승인된 시간 원본에 동기화되어야 함. 클라우드 서비스 공급자가 클라우드 서비스의 일부로 백업 기능을 제공하는 경우 클라우드 서비스 고객은 클라우드 서비스 공급자에게 백업 기능의 사양을 요청해야함. 클라우드 서비스 고객은 백업 요구 사항을 충족하는지 확인하여야 함. 클라우드 서비스 고객은 이벤트 로깅을위한 요구 사항을 정의하고 클라우드 서비스가 이러한 요구 사항을 충족하는지 확인하여야 함.	자원의 사용은 현재 및 예상되는 용량 요구 사항과 일치하도록 지속적으로 모니터링하고 조정함. 정보, 소프트웨어 및 시스템의 백업을 프로젝트별/부서별 정한 주기별로 생성하고, 합의된 백업 주기와 정책에 따라 백업 사본을 안전하게 유지함. 정기적으로 백업을 테스트하여 복원이 원활하게 이루어지는지 확인함. 활동, 예외, 결함 및 기타 관련 이벤트를 기록하는 로그는 정보 보안 정책에 따라 생성되고 저장되며, 이를 통해 시스템 동작의 추적과 이상 징후를 탐지함. 네트워크, 시스템 및 애플리케이션은 비정상적인 동작을 모니터링하고, 즉시 대응하여 잠재적인 정보 보안 사건을 신속하게 처리함. 정보 처리 시스템은 승인된 시간 원본에 동기화되어 정확한 시간 정보를 유지하고 있으며, 클라우드 서비스의 백업 기능은 정확히 검토되어 백업 요구사항이 확실히 충족되도록 활용됨. 클라우드 서비스에서

	클라우드 서비스 사용자는 클라우드 서비스 제공자에게 클라우드 서비스 모니터링 기능의 정보를 요청하여야 함.	발생하는 이벤트 로깅에 대한 요구 사항을 반기별로 업데이트하며 중요 변동이 발생하였을 경우 내부 검토를 통해 바로 변동이 될 수 있도록 함.
응용 프로그램 (ISO/IEC27002 8.18 8.19 ISO/IEC27017 9.4.4 18.1.2)	시스템 및 애플리케이션 제어를 무시할 수 있는 유틸리티 프로그램의 사용은 제한되어야 하며 엄격하게 통제되어야 함. 운영 시스템에 소프트웨어 설치를 안전하게 관리하기 위한 절차와 조치를 구현해야 함. 유틸리티 프로그램 사용이 허용되는 경우 클라우드 서비스 고객은 클라우드 컴퓨팅 환경에서 사용할 유틸리티 프로그램을 식별하고 클라우드 서비스의 제어를 방해하지 않도록하여야 함. 클라우드 서비스 고객은 라이센스가 부여 된 소프트웨어를 클라우드 서비스에 설치하기 전에 클라우드 관련 라이센스 요구사항을 식별하는 절차를 가져야 함.	시스템 및 애플리케이션 제어를 무시할 수 있는 유틸리티 프로그램의 사용을 제한하기 위해 시스템에 설치된 유틸리티 프로그램 목록을 작성하고, 필요한 경우에만 해당 목록을 업데이트하며, 모든 유틸리티 프로그램 사요에 대한 사전 사용 신청 및 승인 프로세스를 취함. 보안 감사 로그를 통해 유틸리티 프로그램 사용 내역을 모니터링하고 불법적인 사용 시 즉각적으로 대응함. 소프트웨어 설치 이전에 해당 소프트웨어의 필요성과 보안 측면에서의 적합성을 평가하고, 운영 시스템에 소프트웨어를 설치하기 위한 변경 관리 절차에 따른 승인이 필요하며, 시스템의 안정성에 미치는 영향을 최소화하기 위해 테스트 환경에서 먼저 시도함. 클라우드 서비스 제어를 방해하지 않도록 API 및 연동 인터페이스를 사용할 때, 해당 서비스의 제어를 방해하지 않도록 정확한 권한과 범위를 설정하고 클라우드 서비스의 이벤트 로그 및 감사 기능을 활용하여 제어에 이상이 생기지 않았는지를 주기적으로 확인하고 모니터링함.