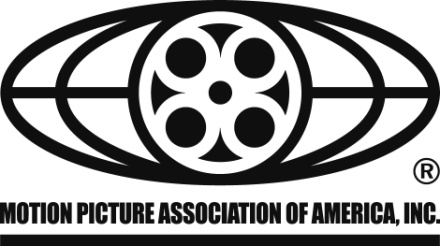
****

**MPAA 콘텐츠 보안 프로그램**

**콘텐츠 보안 모범 사례**

**공통 지침**

[**http://www.mpaa.org/content-security-program/**](http://www.mpaa.org/content-security-program/)

버전 3.0

2015년 4월 2일

문서 이력

|  |  |  |  |
| --- | --- | --- | --- |
| **버전** | **날짜** | **설명** | **작성자** |
| 1.0 | 2009년 12월 31일 | 최초 일반 공개 | Deloitte & Touche LLP  MPAA  MPAA 회원사 |
| 2.0 | 2011년 5월 15일 | 업데이트 및 개정  공통 지침 및 보완 지침으로 통합 | PwC LLP  MPAA  MPAA 회원사 |
| 2.1 | 2013년 1월 1일 | 업데이트 및 개정 | PwC LLP  MPAA  MPAA 회원사 |
| 3.0 | 2015년 4월 2일 | 업데이트 및 개정 | MPAA  MPAA 회원사 |

목차

[문서 이력 i](#_Toc427202204)

[I. 모범 사례 개요 2](#_Toc427202205)

[II. 시설 개요 3](#_Toc427202206)

[III. 위험 관리 4](#_Toc427202207)

[IV. 모범 사례 형식 6](#_Toc427202208)

[V. 모범 사례 공통 지침 7](#_Toc427202209)

[부록 A — 용어집 74](#_Toc427202210)

[부록 B — MPAA 제작물 및 배포 경로 정의 78](#_Toc427202211)

[부록 C - 시설에 대한 매핑 80](#_Toc427202212)

[부록 D - 관리수단의 매핑 참고자료 93](#_Toc427202213)

[부록 E - 자주 묻는 질문 99](#_Toc427202214)

[부록 F - 권장 정책 및 절차 100](#_Toc427202215)

[부록 G - 기타 자료 및 참고문헌 101](#_Toc427202216)

[부록 H - MPAA에 저작권 침해 신고 102](#_Toc427202217)

1. 모범 사례 개요

**소개**

미국영화협회(MPAA, Motion Picture Association of America, Inc.)는 30년이 넘는 기간 동안 회원사(회원)인 Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC, Twentieth Century Fox Film Corporation, Walt Disney Studios Motion Pictures 및 Warner Bros. Entertainment Inc.를 대신하여 콘텐츠 보안 평가를 관리했습니다.

이러한 검토는 표준화된 설문조사 모델, 절차 및 보고서 템플릿을 사용하여 2007년부터 실시되었습니다. 그 이후로 32개국에 있는 약 500개의 시설이 설문 조사에 포함되었습니다.

MPAA는 전세계인들을 대상으로 오락물을 창작하는 이들의 권리를 보호하고자 노력하고 있습니다. 창조 예술에서부터 소프트웨어 산업에 이르기까지 아이디어를 생계 수단으로 삼는 사람의 수가 전세계적으로 늘어나고 있습니다. 이는 곧 지적 재산권을 보호하고 그 보호 수단이 건전한 글로벌 정보 경제의 초석임을 인식하는 것이 점점 중요해지고 있음을 의미합니다.

MPAA 콘텐츠 보안 프로그램은 프로덕션, 포스트 프로덕션, 마케팅 및 배포 단계에 있는 회원사 콘텐츠를 보호하는 절차를 강화하는 데 그 목적이 있습니다. 이러한 강화 방법은 다음과 같습니다.

* 회원사 콘텐츠 보안을 위한 표준 관리방안을 명시한 일련의 시설 서비스별 모범 사례를 발행함
* 발행된 모범 사례를 바탕으로 제3자 협력사의 콘텐츠 보안을 평가 및 산정함
* 회원사 콘텐츠 보안의 중요성을 강조함
* 회원사와 해당 사업 파트너 간의 콘텐츠 보안과 관련하여 별도의 추가 논의를 위한 표준 평가 수단을 제공함

**목적 및 적용 범위**

본 문서는 회원사가 고용한 현재 및 향후의 제3자 업체가 콘텐츠 보안에 대한 일반적인 기대 사항과 현재 발행된 업계 모범 사례를 이해하도록 하는 데 그 목적이 있습니다. 특정 회원사의 업체 이용에 관한 결정은 각 회원사가 일방적으로 정합니다.

콘텐츠 보안을 위한 모범 사례는 시설이 제공하는 서비스, 시설이 취급하는 콘텐츠 종류 및 시설이 속한 개봉 기간을 고려하여 작성됩니다.

본 문서에 설명된 모범 사례는 현지, 주, 지역, 연방 및 국가별 법규의 적용을 받습니다.

본 문서에 설명된 모범 사례, 또는 여기에 포함된 업계 표준, 또는 ISO 참고사항은 정기적으로 변경될 수 있습니다.

**모범 사례의 준수는 전적으로 자유 의사에 따릅니다. 이는 인정 프로그램으로 간주되지 않습니다.**

**예외 절차**

모범 사례의 준수가 실행 불가능한 시설은 준수 불가능 사유를 문서화하고 모범 사례를 대신한 보완책을 실시해야 합니다. 또한 예외 사항은 회원사로 직접 전달해야 합니다.

**질문 또는 의견**

모범 사례에 대한 질문이나 의견은 이메일(contentsecurity@mpaa.org)로 문의하시기 바랍니다.

1. 시설 개요

다음 표에 각 시설 유형마다 일반적으로 제공되는 서비스, 취급 콘텐츠 및 개봉 기간이 설명되어 있습니다.

| **번호** | **시설 유형** | **일반적 시설 서비스** | **콘텐츠 유형** | **개봉 기간** |
| --- | --- | --- | --- | --- |
| **1** | **음성 시설은 제작 과정 중에 녹음되는 음향의 처리와 추가적인 음향 효과 및 악보 제작을 통한 음향의 증강을 담당한다.** | * 원어 및 외국어 더빙 * 자막 제작 * SFX * 음악 제작 * ADR/음향 효과 | * 저해상도 * 워터마크 삽입/스포일링 * 영화 콘텐츠 전체/일부 * 음성 마스터 | * 극장 개봉 전 * 홈비디오 출시 전 |
| **2** | **특송, 배달, 운송** | * 특송 서비스 * 배달 서비스 * 운송 회사 | * 다양 | * 극장 개봉 전 * 홈비디오 출시 전 * 카탈로그 |
| **3** | **크리에이티브 광고** | * 미완성 * 트레일러 * TV 광고 * 티저 광고 * 그래픽 * 웹 광고 | * 워터마크 및 스포일이 삽입된 영화 콘텐츠 전체/일부 * 대본 * 클립 | * 극장 개봉 전 * 홈비디오 출시 전 * 카탈로그 |
| **4** | **디지털**  **영화** | * 디지털 영화 마스터링 * 복사 * 키 관리 | * 고해상도 – 콘텐츠 전체 또는 일부 * 디지털 영화 배포 마스터 * 디지털 영화 패키지 | * 극장 개봉 전 |
| **5** | **디지털**  **서비스** | * 디지털 후반 작업 * 스캔 * 필름 녹화 * 필름 복원 | * 클린 및 고해상도 – 콘텐츠 전체 또는 일부(필름 테이프) | * 극장 개봉 전 * 카탈로그 |
| **6** | **배포** | * 배포 * 이행 * 필름 창고 * DVD/테이플 재활용 | * 고해상도 * 클린 영상 | * 극장 개봉 전 * 홈비디오 출시 전 * 카탈로그 |
| **7** | **DVD**  **제작** | * 압축 * 저작 * 엔코딩 * 지역화 * 부가 영상 * 디스크 QC 검사 | * 클린 – 영화 전체 | * 홈비디오 출시 전 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 주제** | **개괄적 설명** | **일반적 시설 서비스** | **비디오 특성** | **개봉 기간** |
| **8** | **DVD**  **제작** | * 압축 * 저작 * 엔코딩 * 지역화 * 부가 영상 * 디스크 QC 검사 | * 클린 – 영화 전체 | * 출시 전 * 홈비디오 |
| **9** | **기내 오락(IFE) 및**  **접객 서비스** | * IFE 현상소 * IFE 통합 * 호텔 * 항공 * 유람선/여객선 * 도서관 * 병원 * 교도소 | * 고해상도 – 콘텐츠 전체 또는 일부 * 스포일링 – 콘텐츠 전체 또는 일부 | * 극장 개봉 전 * 홈비디오 출시 전 * 카탈로그 |
| **10** | **후반 제작 서비스** | * 텔레시네 * 복제 * 편집 * 마감 * QC | * 고해상도 – 콘텐츠 전체 또는 일부 | * 극장 개봉 전 * 홈비디오 출시 전 * 카탈로그 |
| **11** | **복사** | * 예비 마스터링 * 마스터링 * 복사 * 디스크 제작 검사 | * 고해상도 * 클린 영상 | * 홈비디오 출시 전 |
| **12** | **시각**  **효과**  **(VFX)** | * 디지털 후반 제작 * 컴퓨터합성영상(CGI) * 애니메이션 | * 고해상도 – 일부 * 프레임, 샷, 시퀀스 및 스틸 * 대본 * 스토리보드 | * 극장 개봉 전 * 극장 개봉 후(2D에서 3D로) |
| **13** | **응용 프로그램** | * 응용 프로그램 개발 | * 다양 | * 다양 |
| **14** | **클라우드** | * 호스팅 * 데이터 센터 | * 다양 | * 다양 |

1. 위험 관리

**위험 평가**

위험은 위험 평가를 통해 식별해야 하며 허용 가능한 수준까지 위험을 줄이는 한편 사업 목표를 달성할 수 있도록 적절한 관리수단을 구현해야 합니다.

국제표준화기구(ISO) 27000은 위험을 “사고 확률 및 그 결과의 조합”으로 정의합니다. 예를 들어, 콘텐츠가 시설 네트워크로부터 도난 되어 일반에 공개될 확률과 이러한 사고가 발생할 경우 조직 및 그 고객에게 미치는 사업상 결과(예: 계약 위반 및/또는 해당 개봉 기간 중의 수익 손실)입니다.

견고한 관리 체계의 중요성은 ISO 27001 표준에도 강조되어 있습니다. 이 표준은 정보보호 관리체계(ISMS)를 수립하는 방법을 제시합니다.

**자산 분류**

시설의 자산을 분류하는 한 방법은 아래에 요약된 4단계 절차를 따르는 것입니다.

효과 모니터링 및 평가

최소 보안 관리수단 결정

관리수단 구현

자산 식별 및 분류

조직은 회원사(해당 고객)와 상의하여 보다 높은 수준의 보안이 필요한 고객 자산을 판단할 책임이 있습니다. 다음 표에 콘텐츠를 분류하는 방법의 예가 나와 있습니다.

| **분류** | **설명** | **예** |
| --- | --- | --- |
| **고도의 보안이 필요한 콘텐츠** | 조직이 판단하기에 자산이 도난되거나 유출될 경우 금전적 손실, 부정적인 브랜드 평판, 또는 심각한 처벌로 이어질 수 있는 콘텐츠 | * 전세계 첫 극장 개봉 전 블록버스터 영화의 도난 * 전세계 첫 출시일 전 홈비디오 콘텐츠의 도난 * 마스터 또는 스크리너의 도난 |

각 시설 유형과 관련된 일반적 위험에 대한 추가 정보는 각 모범 사례 보완 문서에 포함되어 있습니다.

**보안 관리수단**

정보기술관리협회(ITGI)는 관리수단을 “사업 목표를 달성하고 유해 사고를 예방 또는 감지하여 수정할 수 있는 합리적인 확실성을 제공하도록 마련된 정책, 절차, 실천안 및 조직 체계”로 정의합니다. 보안 관리수단은 보통 자산의 분류, 자산이 조직에 제공하는 가치 및 자산의 유출이나 도난 위험을 바탕으로 선택합니다.

식별된 위험을 완화할 수 있도록 조직이 구체적인 각 위험에 알맞은 관리수단을 시행할 것을 권장합니다. 또한 현재의 위협 환경에 근거하여 그러한 조치의 계획 및 효과를 정기적으로 평가해야 합니다.



**관리 시스템**



**역량**



**디지털 보안**



**인프라**



**자산 관리**



**조직 및 관리**



**콘텐츠 관리**



**IV. 문서 구성**



**MS-1 임원의 보안 인식/감독 페이지 7**

**모범 사례는 고객의 콘텐츠를 보호할 수 있는 시설의 능력을 평가하는 체계를 제시하는 MPAA 콘텐츠 보안 모델에 따라 구성되어 있습니다. 또한 관리 시스템, 물리적 보안 및 디지털 보안의 3가지 영역에 대한 보안 주제로 구성되어 있습니다. MPAA 콘텐츠 보안 모델의 구성 요소는 관련 ISO 표준(27001/27002), 보안 표준(즉, NIST, CSA, ISACA 및 SANS) 및 업계 모범 사례를 참고하여 작성되었습니다.**

**MS-2 위험 관리 페이지 7**

**MS-3 보안 조직 페이지 8**

**MS-4 정책 및 절차 페이지 9**

**MS-5 사고 대응 페이지 12**

**MS-6 사업 연속성 및 재해 복구 페이지 14**

**MS-7 변경 제어 및 구성 관리 페이지 15**

**MS-8 워크플로우 페이지 15**

**MS-9 업무 분장 페이지 16**

**MS-10 신원 조회 페이지 17**

**MS-11 기밀유지 계약 페이지 17**

**MS-12 제3자 이용 및 적격심사 페이지 18**

**PS-1 출입 지점 페이지 20**

**PS-2 방문객 출입 페이지 21**

**PS-3 신분 확인 페이지 22**

**PS-4 경계 보안 페이지 22**

**PS-5 경보 페이지 23**

**PS-5 권한 부여 페이지 25**

**PS-8 열쇠 페이지 26**

**PS-9 카메라 페이지 28**

**PS-7 전자식 출입 제어 페이지 25**

**PS-10 로깅 및 모니터링 페이지 29**

**PS-11 수색 페이지 30**

**자산 관리**

**PS-12 재고 추적 페이지 33**

**PS-13 재고 합계 페이지 34**

**PS-14 공백 매체/생필름 추적 페이지 35**

**PS-15 고객 자산 페이지 35**

**PS-16 처분 페이지 36**

**PS-17 운송 페이지 38**

**PS-18 수취 페이지 39**

**PS-19 라벨 부착 페이지 40**

**PS-20 포장 페이지 40**

**PS-21 수송 차량 페이지 41**

**DS-1 방화벽/WAN/경계 보안 페이지 42**

**DS-2 인터넷 페이지 46**

**DS-3 LAN/내부 네트워크 페이지 48**

**DS-4 무선 페이지 51**

**DS-5 입출력 장치 보안 페이지 53**

**DS-6 시스템 보안 페이지 53**

**DS-7 계정 관리 페이지 56**

**DS-7.7-8.4 인증 페이지 58-60**

**DS-9 로깅 및 모니터링 페이지 61**

**콘텐츠 전송**

**DS-10 모바일 보안 페이지 63**

**콘텐츠 전송**

**DS-11 보안 기술 페이지 65**

**DS-12 콘텐츠 추적 페이지 67**

**DS-13 전송 시스템 페이지 68**

**DS-14 전송 장치 방법론 페이지 68**

**DS-15 고객 포털 페이지 70**

1. 모범 사례 형식

모범 사례는 다음 형식을 사용하여 MPAA 콘텐츠 보안 모델에 포함된 각 보안 주제에 대해 제시됩니다.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 관리 시스템 | 물리적 보안 | | | 디지털 보안 | | |
| 조직 및 관리 | 시설 | 자산 관리 | 운송 | 인프라 | 콘텐츠 관리 | 콘텐츠 전송 |

모든 페이지 상단에 있는 차트는 전체 MPAA 콘텐츠 보안 모델 내에서 다루어지고 있는 보안 영역을 강조해서 보여줍니다.

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| PS-9.0 | 열쇠 | **마스터 열쇠**는 오직 권한 있는 관계자(예: 소유자, 시설 관리 팀)에게로 배포를 제한한다 | * **마스터 열쇠**를 빌릴 수 있도록 허용된 **회사 관계자** 목록을 작성, 유지한다 * 해당 목록을 정기적으로 업데이트하여 **마스터 열쇠** 사용이 더 이상 필요하지 않은 **회사 관계자**를 목록에서 삭제한다 |
| PS-9.1 | **마스터 열쇠**의 배포를 추적 및 감시할 수 있는 대여/반환 절차를 실시한다 | * 기록을 유지하여 다음 정보를 추적한다. * **각 마스터 열쇠**를 소유하고 있는 **회사 관계자** * 대여/반환 시간 * 대여 사유 |

P

**용어집**

용어집에 포함된 모든 용어는 **굵은 글씨체**로 표시되며 부록 A에 정의되어 있습니다.

**이행 지침**

조직의 모범 사례 구현을 돕도록 추가 고려사항, 가능한 시행 단계 및 예가 제공됩니다.

**모범 사례**

모범 사례는 각 보안 주제에 대해 설명되어 있습니다.

**보안 주제**

각 역량 부분은 하나 이상의 “보안 주제”로 구성됩니다. 각 보안 주제에 대해 하나 이상의 모범 사례가 제시됩니다.

**번호**

각 모범 사례에는 XX-Y.Z 형태의 참조 번호가 할당됩니다. XX는 일반 영역, Y는 보안 주제, Z는 특정 관리수단을 가리킵니다.

1. 모범 사례 공통 지침

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-1.0 | 운영진의 보안 인식/감독 | 사업주/고위 경영진으로부터 승인 받은 정보 보안을 위한 관리수단 체계를 구현하는 정보 보안 관리 시스템을 확보한다. | * 예: ISO27001의 ISMS 프레임워크, NIST, CoBIT 등 |
| MS-1.1 | 최소한 1년에 한 번 정보 보안 관리 정책과 절차를 검토한다. |  |
| MS-1.2 | 최소한 1년에 한 번 회사의 콘텐츠 보안 책임에 대해 운영진/소유자를 교육하고 참여하게 한다. |  |
| MS-1.3 | 정보 보안 관리 정책을 수립하고 검토할 정보 보안 관리 그룹을 만든다. |  |
| MS-2.0 | 위험 관리 | 시설과 관련된 콘텐츠 도난 및 유출의 위험을 식별하고 그 우선순위를 정하기 위해 콘텐츠 워크플로우 및 민감한 자산에 중점을 둔 공식적으로 문서화된 보안 위험 평가 절차를 개발한다. | * 보안 **위험 평가**에 대한 명확한 범위를 정의하고 필요에 따라 수정한다. * 위험 발생 가능성, 사업 목표/콘텐츠 보호에 미치는 영향 및 우선순위 할당을 위한 자산 분류를 포함하는 체계적 접근 방법을 적용한다. * 문서화된 **워크플로우**와 관련된 모범 사례는 MS-6.0 참조한다. |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-2.1 | 위험 관리 | 내부 **위험 평가**를 연례적으로 실시할 뿐만 아니라 최소 요건인 MPAA 모범 사례 공통 지침과 적용 가능한 보완 지침을 바탕으로 워크플로우 주요 사항이 변경된 경우에도 실시하며 식별된 위험을 문서화하고 이에 대해 조치한다. | * 최소한 분기마다 경영진과 주요 이해관계자가 참석하는 회의를 열어 콘텐츠 도난 및 유출 위험을 식별하고 문서화한다 * DS-1.8 및 DS-1.9에 따라 분기마다 외부 및 내부 네트워크 취약성 검사 및 외부 침투 테스트를 수행한다. * 시설측이 판단하기에 콘텐츠 손실이 발생할 수 있는 부분을 반영하는 주요 위험을 식별한다. * 관리수단을 구현, 문서화하여 식별된 위험을 완화하거나 줄인다. * 최소한 분기마다 개선 활동 및 구현된 관리수단의 효과를 모니터링 및 평가한다. * 보안 계획, 업그레이드 및 유지관리에 대해 문서화하고 예산을 편성한다. |
| MS-3.0 | 보안 조직 | 연락처의 주요 보안 접점을 식별하고 콘텐츠 및 자산 보호에 대한 역할과 책임을 공식적으로 정의한다. | * 조직표와 직무 기술서를 마련하여 콘텐츠 보안과 관련한 역할과 책임 사항의 지정을 촉진한다. * 자신의 직무와 관련된 정책 및 절차에 대해 보안 인력이 준비할 수 있도록 온라인 또는 현장 교육을 제공한다. |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-4.0 | 정책 및 절차 | 자산 및 콘텐츠 보안에 대한 정책과 절차를 수립한다. 정책은 최소한 다음 주제를 다루어야 한다.   * 수용 가능한 사용(예: 소셜 네트워킹, 인터넷, 전화, 개인 장치, 모바일 장치 등) * 자산 및 콘텐츠의 분류 및 취급 정책 * 사업 연속성(백업, 보존 및 복원) * 변경 제어 및 구성 관리 정책 * 기밀유지 정책 * 디지털 기록 장치(예: 스마트폰, 디지털 카메라, 캠코더) * 예외 정책(예: 문서화 절차 정책의 예외) * 사고 대응 정책 * 모바일 장치 정책 * 네트워크, 인터넷 및 무선 정책 * 비밀번호 관리수단(예: 비밀번호 최소 길이, 화면보호기) * 보안 정책 * 방문객 정책 * 징계/제재 정책 * 콘텐츠의 저작권 침해 또는 부적절한 취급을 익명으로 보고하는 내부적인 방법(예: 상담 전화 또는 이메일 주소) | * 정책 및 절차를 개발할 때 특정 시설/비즈니스 워크플로우를 고려한다. * 모든 정책과 절차는 발행 및 공개되기 전에 운영진이 서명하도록 요구한다. * 신입 사원 오리엔테이션 교육 시 징계 조치에 대해 전달한다. * 고려할 만한 정책 및 절차의 목록은 부록 F를 참조한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| MS-4.1 | 정책 및 절차 | 최소한 1년에 한 번 보안 정책 및 절차를 검토 및 업데이트한다. | * 보안 정책 및 절차에 대한 연례 운영진 검토에 다음 요인을 포함시킨다. * 최근 보안 추세 * 회사 관계자의 피드백 * 새로운 위험 및 취약점 * 규제기관(즉, FTC 등)의 권고 사항 * 이전의 보안 사고 |
| MS-4.2 | 모든 **회사 관계자**(예: 정직원, 임시 직원, 인턴) 및 **제3자 근무자**(예: 계약직원, 프리랜서, 파견업체)와 모든 현재 정책, 절차 및/또는 고객 요구사항에 대해 커뮤니케이션하고 서명을 요구한다. | * **회사 관계자** 및 **제3자 근무자**의 신규 채용 시 모든 일반 정책과 절차가 포함된 회사 안내책자 사본을 제공한다. * **회사 관계자** 및 **제3자 근무자**에게 보안 정책, 절차 및 고객 요구사항에 대해 공지한다. * 경영진은 모든 **회사 관계자** 및 **제3자 근무자**에 대한 현재 정책, 절차 및 고객 요구사항의 서명을 보존해야 한다. |
| MS-4.3 | 정책 및 절차 | 보안 정책 및 절차에 대한 인식 프로그램을 개발하고 정기적으로 업데이트한다. 그리고 채용 시 및 채용 후 연례적으로 **회사 관계자** 및 **제3자 근무자**에게 최소한 다음 부분과 관련된 보안 정책 및 절차를 교육한다.   * IT 보안 정책 및 절차 * 일반 및 특정 고객이 요구하는 콘텐츠/자산 보안 및 취급 방법 * 보안 사고 보고 및 상달 * 징계 정책 * 암호화된 콘텐츠를 취급하는 모든 개인의 암호화 및 키 관리 * 자산 처분 및 파기 절차 | * 경영진/직원 회의 동안 보안 인식 메시지를 전달한다. * 어떤 **회사 관계자**가 연례 보안 교육(예: 데이터베이스 저장소, 참석자 로그, 수료증)을 이수했는지 추적하는 절차를 구현한다. * 채용 시 온라인 또는 오프라인 교육을 제공하여 **회사 관계자** 및 **제3자 근무자**에게 일반적인 사고, 그에 상응하는 위험 및 감지된 사고를 보고해야 하는 책임에 대해 교육한다. * 포스터, 이메일 및 정기적인 뉴스레터와 같은 보안 인식 자료를 배포하여 보안 인식을 강화한다. * 저작권 침해 문제를 완화하기 위해 직무 및 민감한 콘텐츠(예: IT 인력, 제작)와의 상호작용에 기반하여 맞춤형 메시지와 교육을 개발한다. * 교육 세션을 녹화하여 참조용으로 활용할 수 있도록 만드는 것을 고려한다. |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-5.0 | 사고 대응 | 보안 사고가 탐지되어 보고된 경우 취해야 할 조치를 설명하는 공식 사고 대응 계획을 수립한다. | * **사고 대응** 계획에 다음 사항이 포함되도록 고려한다. * 사고의 정의 * 보안 팀에게 알림 * 운영진에게 상달 * 영향 및 우선순위 분석 * 영향 억제 * 제거 및 복구 * 핵심 연락처 정보(고객 스튜디오 연락처 정보 포함) * 영향을 받는 사업 파트너 및 고객의 통지 * 사법당국의 통지 * 사고 세부사항의 보고 * 컴퓨터 보안 사고 처리는 NIST SP800-61 개정 2를 참조한다 |
| MS-5.1 | 보안 사고의 탐지, 분석, 교정을 담당하는 보안 사고 대응 팀을 구성한다. | * 모든 종류의 보안 사고를 다룰 수 있도록 다양한 직무 대표를 포함시킨다. 다음 사항을 고려한다. * 관리 * 물리적 보안 * 정보 보안 * 네트워크 팀 * 인사 * 법무 * **사고 대응** 팀원들이 사고 처리에 대한 자신의 역할과 책임 사항을 이해할 수 있도록 교육을 제공한다. |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-5.2 | 사고 대응 | 개인이 보안 **사고 대응** 팀에게 탐지된 사고를 보고할 수 있도록 보안 사고 보고 절차를 수립한다. | * 부적절 및/또는 수상한 활동을 보고하는 데 이용할 수 있는 익명의 상담전화나 웹사이트의 구현을 고려한다. * 사고 대응 팀의 모든 팀원에게 정보를 알릴 수 있는 사고 보고용 그룹 이메일 주소를 만드는 것을 고려한다. * 수상한 활동에 대한 익명의 제보가 가능하도록 MPAA 제보 전화의 활용을 고려한다 - 부록 H에 있는 상시 제보 전화 연락처를 참조한다. |
| MS-5.3 | 소유 콘텐츠가 유출 또는 도난 되거나, 기타 위험(예: 고객 자산이 사라짐)에 노출된 고객에게 신속히 사고를 알리고 운영진 및 고객이 참석하는 사후 회의를 소집한다. | * 위반 통지 양식의 사용을 포함한 보안 위반 통지 절차를 구현한다. * 해당 고객에게 콘텐츠 손실을 보고할 때 취해야 할 수정 조치를 결정할 수 있도록 법무 팀을 참여시킨다. * 사고에서 얻은 교훈을 논의하고 사고 대응 계획과 절차에 대한 개선 방안을 파악한다. * 근본 원인 분석을 실시하여 사고 발생의 원인이 된 보안 취약점을 식별한다. * 유사한 사고가 다시 발생하지 않도록 방지할 수 있는 교정 조치를 식별 및 구현한다. * 교정 조치 계획을 포함한 사후분석 결과를 해당 고객에게 전달한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| MS-6.0 | 사업 연속성 및 재해 복구 | 사업 연속성을 보장하기 위해 취해진 조치를 설명하는 공식 계획을 수립한다. | * **사업 연속성** 계획에 다음 섹션을 포함시킬 것을 고려한다. * 전력 및 통신 중단, 시스템 장애, 자연 재해 등을 포함하는 중요 자산 및 콘텐츠에 대한 위협 * 중요 WAN 및 LAN/내부 네트워크 장치의 구성을 포함하여 세부적인 정보 시스템, 콘텐츠 및 메타데이터 백업 절차 및 정보 시스템 문서화 * 백업의 암호화(최소 AES-128비트 암호화) * 중요 시스템의 안전한 종료를 수행하는 소프트웨어를 포함하여 CCTV 시스템, 경보 및 중요 정보 시스템에 최소 15분 동안 지원할 수 있는 백업 전원 공급 * 오프사이트 백업 위치의 사용을 고려한다. * 보안 팀에게 알림 * 운영진에게 상달 * 영향 및 우선순위 분석 * 영향 억제 * 복원된 시스템의 수동 해결 방법 및 구성 세부사항을 포함하여 복원 우선순위 및 세부적인 복원 절차 * 주요 연락처 정보 * 영향을 받는 사업 파트너 및 고객의 통지 * 최소한 1년에 한 번 사업 연속성 및 재해 복원 절차의 테스트 |
| MS-6.1 | 연속성 사고를 감지, 분석 및 교정을 담당할 사업 연속성 팀을 구성한다. | * 정의된 역할 및 책임을 포함한다. * 사업 연속성 팀원이 각자의 역할과 책임을 이해하도록 교육을 제공한다. |
| MS-7.0 | 변경 제어 및 구성 관리 | 새로운 데이터, 응용 프로그램, 네트워크 및 시스템 구성요소가 회사 리더의 사전 승인을 받았는지 확인할 정책 및 절차를 수립한다. | * 장치, 서비스 및 기능의 설치, 구성 및 사용을 설명하는 문서를 포함하고 필요에 따라 문서를 업데이트한다. * 알려진 문제를 처리할 정책 및 절차를 문서화한다. * 버그와 보안 취약성을 보고할 정책 및 절차를 포함한다. * 비인가 하드웨어 또는 소프트웨어의 설치를 제한 및 모니터링한다. * 데이터, 응용 프로그램, 네트워크 인프라 및 시스템에 대한 변경과 관련된 위험을 관리한다. * 모든 변경 요청, 테스트 결과 및 경영진 승인을 문서화 및 보존한다. |
| MS-8.0 | 워크플로우 | 콘텐츠 및 승인 지점을 추적하는 **워크플로우**를 문서화한다. 물리적 및 디지털 콘텐츠 모두에 다음 절차를 포함한다:   * 전달(수취/반환) * 입수 * 이동 * 보관 * 제거/파기 | * 스윔 레인 다이어그램을 사용하여 **워크플로우**를 문서화한다. * 해당되는 경우 자산 처리 및 취급 정보를 포함한다. * 각 접점에서 콘텐츠에 대한 위험을 평가한다. * 승인 지점 주위에 관리수단을 구현한다. * 관련된 응용 프로그램 관리수단을 식별한다. |
| MS-8.1 | 절차가 변경될 때 **워크플로우**를 업데이트하고 최소한 1년에 한 번 **워크플로우** 절차를 검토하여 변경 사항을 식별한다. | * 취약한 부분을 파악할 수 있도록 콘텐츠 **워크플로우**를 따르고 각 절차에 대해 관리수단을 구현한다. |
| MS-9.0 | 업무 분장 | 콘텐츠 **워크플로우** 내에서 업무를 분장한다. 분장이 현실적이지 않은 경우 보상 관리수단을 구현하고 문서화한다. | * 역할 및 책임 사항을 문서화하여 다음의 역할 기반 직무가 겹치지 않도록 한다. * **금고실** 및 서버/장비실 담당자 * 운송 및 수취 담당자 * **금고실** 및 콘텐츠/제작 영역으로부터 시설 내 다른 장소로 자산 이전(예: 식음료 운반 담당자) * **디지털 자산** 폴더 접근(예: 데이터 취급 담당자가 프로듀서가 사용할 접근 권한을 설정함) * 제작진 중 콘텐츠 전송 담당자 * 수동적 관리수단(예: 콘텐츠 작업 전에 프로듀서가 승인함) 또는 작업지시 시스템의 자동화된 관리수단(예: **워크플로우** 각 단계에 대한 자동화된 승인)을 사용하여 업무를 분장한다. * 분장이 달성 가능하지 않은 경우 다음과 같은 보완 관리수단을 구현한다. * 회사 관계자 및/또는 제3자 근무자의 활동을 모니터링한다. * 감사 기록지를 유지, 검토한다. * 분장을 물리적으로 구현한다. * 임원이 감독하게 한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| MS-10.0 | 신원 조회 | 모든 **회사 관계자** 및 **제3자 근무자**에 대해 배경 적격심사를 실시한다. | * 관련 법률, 규정, 조합 내규 및 문화적 고려사항에 맞춰 신원 조회를 수행한다. * 업무 요구사항, 사용 대상 콘텐츠의 민감도 및 콘텐츠 도난이나 유출의 잠재적 위험에 비례한 배경 적격심사를 통해 잠재적인 **회사 관계자** 및 **제3자 근무자**를 선별한다. * 필요한 경우, 신원, 학력 및 전문 자격을 조회한다. * 법에 의해 신원 조회가 허용되지 않는 경우, 예외 사항으로 문서화하고 평판 조회를 활용한다. |
| MS-11.0 | 기밀유지 계약 | 채용 시 및 채용 이후 연례적으로 콘텐츠 취급 및 보호와 관련된 요구사항을 포함한 기밀유지 계약(예: 비공개 계약)에 모든 **회사 관계자**와 제3자 근무자가 서명하도록 한다. | * 고용, 계약, 또는 합의 종료 후의 기밀유지와 관련된 비공개 지침을 포함시킨다. * 필요에 따라 기밀유지/비공개 계약의 중요성을 일반적인 비법률 용어로 설명한다. * **회사 관계자**가 사업과 관련된 민감한 콘텐츠를 취급하는 데 사용한 기기에 대한 모든 관련 정보를 해당 조직으로 전송하고 기기로부터 안전하게 삭제하도록 한다. * 경영진은 모든 **회사 관계자**가 서명한 기밀유지 계약을 보존해야 한다. |
| MS-11.1 | 소유 중인 모든 콘텐츠와 고객 정보는 고용 또는 계약 종료 시 반환하도록 모든 **회사 관계자**에게 요구한다. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-12.0 | 제3자의 이용 및 적격심사 | 콘텐츠를 취급하는 모든 **제3자 근무자**가 고용 시 기밀유지 계약(예: 비공개 계약)에 서명하도록 요구한다. | * 고용, 계약, 또는 합의 기간이나 기간 종료 후의 기밀유지와 관련된 비공개 지침을 정책에 포함시킨다. * 필요에 따라 기밀유지/비공개 계약의 중요성을 일반적인 비법률 용어로 설명한다. * **제3자 근무자**가 사업과 관련된 민감한 콘텐츠를 취급하는 데 사용한 기기에 대한 모든 관련 정보를 해당 조직으로 전송하고 기기로부터 안전하게 삭제하도록 한다. * 경영진은 모든 **제3자 근무자**가 서명한 기밀유지 계약을 보존해야 한다. * 콘텐츠 취급 및 보호에 대한 요구사항을 포함한다. |
| MS-12.1 | 소유 중인 모든 콘텐츠와 고객 정보는 고용 또는 계약 종료 시 반환하도록 모든 **제3자 근무자**에게 요구한다. |  |
| MS-12.2 | 제3자 계약에 보안 요구사항을 포함시킨다. | * 제3자 계약 및 고객 요구사항에 명시된 보안 요구사항을 **제3자 근무자**가 준수하도록 요구한다. * 민감한 콘텐츠가 관련된 활동에 대한 감사권 조항에 대한 권리를 포함시킨다. * 보안 요구사항의 준수에 대한 모니터링 절차를 구현한다. |
| MS-12.3 | 관계 종료 시 **콘텐츠**를 회수할 절차를 구현한다. | * 제3자 기기에 대한 모든 **콘텐츠**를 해당 조직으로 전송하고 기기로부터 안전하게 삭제하도록 한다. |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| MS-12.4 | 제3자의 이용 및 적격심사 | 적절한 경우 **제3자 근무자**가 보증 및 보험에 들도록 요구한다(예: 특송 서비스). | * **제3자 근무자**가 보험 증서를 제시하도록 하고 해당 보험 제공자 및 보험증권 번호에 대한 기록을 보관하도록 요구한다. * 제3자 보험이 특정한 보험 적용 수준을 만족하도록 요구한다. * 계약이 갱신될 때 매년 정보를 업데이트하도록 요구한다. |
| MS-12.5 | 직무에 필요한 경우가 아니면 콘텐츠/제작 영역에 대한 제3자 접근을 제한한다. | * **제3자 근무자**가 콘텐츠 보관 영역에 대해 전자식 출입 권한을 갖지 않도록 한다. * **제3자 근무자**(예: 청소 직원)가 제한 구역(예: **금고실**)에 접근해야 하는 경우 동행한다. |
| MS-12.6 | 콘텐츠를 취급하기 위해 **하도급 업체**를 이용하거나 다른 회사로 작업을 분담하는 경우 고객에게 통지한다. | * 서면 고객 서명/승인을 요구한다. * 하도급 업체가 표준 **실사** 활동을 통과하도록 요구한다. * 다른 회사로 분담된 작업은 MPAA 회원 스튜디오에 보고되어야 하고 MPAA 업체 질문지를 작성해야 하며 실사 결과를 회원 스튜디오에 제공해야 한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| PS-1.0 | 출입 지점 | 적재 구역 문과 창문을 포함하여 시설의 모든 출입 지점은 항상 보안 장치를 사용한다. | * 접견 공간이 제한 출입문에 의해 나머지 시설과 분리된 경우 업무 시간 중에 출입 지점을 잠금 해제하도록 허용한다. |
| PS-1.1 | 기타 시설 영역(예: 관리 사무소, 대기실, 적재 구역, 특송 집배 및 배달품 전달 영역, 복사 및 마스터링)에서 콘텐츠 영역을 분리하여 콘텐츠가 취급되는 영역에 대한 접근을 제어한다. | * 알 필요가 있는 경우에만 콘텐츠/제작 구역의 접근을 허용한다. * 상영 목적으로 사용되는 공간(예: 영사실)은 접근을 제한하도록 요구한다. * **매체** 재생기(예: Blu-ray, DVD)가 있는 공간에 대한 접근을 제한한다. * 복사 및 마스터링 룸 모두에 대한 접근 권한을 한 사람으로 제한하는 업무 분장 모델을 의무화한다. |
| PS-1.2 | 다음을 포함하지만 이에 국한되지 않는 한 시설 내에 공동 할당된 업무가 있는 상황의 접근을 제한한다.   * 업무 영역 분장 * 사업부에 따라 나누어질 수 있는 접근이 통제된 입구 및 출구 구현 * 시설 내의 모든 입구와 출구의 로깅 및 모니터링 * 시설 내의 모든 임차인은 고용 전에 고객에게 보고되어야 함 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| PS-2.0 | 방문객 출입 | 상세한 방명록을 유지하고 다음 사항을 포함한다.   * 트랙터 및 트레일러의 번호판 * 회사 * 입장시간/퇴장시간 * 방문 대상 * 방문객 서명 * 할당된 명찰 번호 | * 사진이 부착된 유효한 신분증(예: 운전면허증, 정부 발행 신분증)을 제시하도록 요구하여 모든 방문객의 신원을 확인한다. * 이전 방문객의 이름이 보이지 않게 할 수도 있다. |
| PS-2.1 | 각 방문객에게 **신분 확인증**이나 스티커를 할당하여 항상 눈에 띄도록 착용하게 하고 출구에서 확인증을 수거한다. | * 방문객 명찰이 **회사 관계자** 명찰과 쉽게 구분되도록 한다(예: 색깔로 구분된 플라스틱 명찰). * 종이 명찰이나 스티커 색깔을 일별로 교대할 수도 있다. * 만료 시 색깔이 변하는 명찰을 사용할 수도 있다. * 입장/퇴장 시 명찰 할당을 기록한다. * 방문객 명찰은 일련 번호로 매겨 추적해야 한다. * 명찰의 소재는 매일 파악한다. |
| PS-2.2 | 방문객에게 콘텐츠/제작 구역에 대한 키 카드 출입 권한을 제공하지 않는다. |  |
| PS-2.3 | 방문객이 시설 내 또는 콘텐츠/제작 구역에 있는 동안 권한 있는 직원이 방문객과 동행하도록 요구한다. |  |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| PS-3.0 | 신분 확인 | **회사 관계자** 및 장기 고용된 **제3자 근무자**(예: 경비인)에게 유효한 사진 부착 **신분 확인증**을 제공하고 항상 눈에 띄게 착용하도록 한다. | * 신원 조회가 완료된 후 모든 **회사 관계자** 및 장기 고용된 **제3자 근무자**에게 사진이 부착된 **신분 확인증**을 발급한다. * 고용 종료 시 사진이 부착된 **신분 확인증**을 즉시 회수하는 절차를 수립 및 구현한다. * 사진이 부착된 **신분 확인증**에서 위치, 회사 이름, 로고 및 기타 특정 정보를 제외하는 것을 고려한다. * 가능한 경우 사진이 부착된 **신분 확인증**을 출입 키 카드로 사용할 수 있다. * 분실 또는 도난된 사진 부착 **신분 확인증**은 즉시 신고하도록 직원들에게 요구한다. * 분실 또는 도난된 사진 부착 **신분 확인증**을 신고할 수 있는 상시 운영 전화번호 또는 웹사이트를 제공한다. * 직원들이 확인증이 보이지 않는 사람을 검문하도록 교육 및 권장한다. |
| PS-4.0 | 경계 보안 | 조직의 **위험 평가**에 의해 식별되어 시설에 노출될 수 있는 위험을 해결하는 경계 보안 관리수단을 구현한다. | * 시설의 위치 및 배치에 기반하여 다음과 같은 보안 관리수단을 구현한다. * 최소한 업무 외 시간 동안 보안이 유지되는 벽, 울타리 및/또는 출입문 사용을 통해 경계 접근을 제한한다. 벽/울타리는 약 8피트(2.4m) 이상이 되어야 한다. * 필요에 따라 흡연 구역 및 개방 발코니 등의 공동 외부 구역의 보안 유지 및 경계 설정 * 공동 외부 구역(예: 흡연 구역)과 주차 공간을 충분히 포괄하는 외부 카메라의 촬영 범위 * 표적이 될 수 있는 회사 간판의 과도한 사용에 대한 주의 * 필요에 따라 경계 주위에 경보기 사용 |
| PS-4.1 | 경계 입구와 일반 출입구 지점에 보안 요원을 배치한다. |  |
| PS-4.2 | 경계 보안 | 일일 불시 보안 순찰 절차를 구현하고 순찰 결과를 로그로 문서화한다. | * 보안 요원이 내/외부 영역을 순찰한다. * 봉인물 확인을 포함하여 비상구 검사를 포함시킨다. * 순찰(예: 검사 지점)을 추적하고 잠금을 확인하는 보안 요원 순찰 시스템을 사용할 수도 있다. |
| PS-4.3 | 경계 출입문을 항상 잠근다. | * 시설로의 차량 접근을 제어하기 위해 보안 요원에 의해 조작되는 전자식 차단기를 구현한다. * 적절한 서류 절차를 완료한 회사 관계자 및 제3자 근무자에게 주차증을 배포한다. * 방문 차량이 신분증을 제시하도록 요구하고 구내 출입 시 모든 방문객이 사전 허가를 받도록 한다. |
| PS-5.0 | 경보 | 모든 출입 지점(비상구 포함), 창문, 적재 구역, 화재 대피용 계단 및 제한 구역(예: **금고실**, 서버/장비실)을 커버하는 집중식 가청 경보 시스템을 설치한다. | * 시설 내 무단 진입에 대해 보안 요원에게 알릴 수 있도록 모든 출입구에 경보기를 설치한다. * 시설이 감독되지 않을 때 경보를 활성화한다. |
| PS-5.1 | 제한 구역(예: **금고실**, 서버/장비실)에 동작 감지기를 효과적으로 설치 및 배치하고 적절한 보안 요원과 기타 관계자(예: 프로젝트 관리자, 프로듀서, 편집장, 사고 대응 팀 등)에게 경보하도록 구성한다. | * 한층 추가된 보안책으로서, 정상 업무 시간 이후 경보 시스템의 작동 범위에 동작 감지기 등을 통해 보관 구역 및 **금고실**이 포함되도록 한다. |
| PS-5.2 | 민감한 출입 지점이 사전 설정된 시간(예: 60초)보다 오래 열려 있을 경우 통보하도록 콘텐츠/제작 구역에 출입문 지지 경보기를 설치한다. | * 출입문이 지지 장치에 의해 장시간 열린 상태로 있을 경우 경보를 발하고 보안 담당자에게 통보할 수 있도록 접근 통제 출입문을 구성한다. |
| PS-5.3 | 경보 | 보안 담당자와 기타 관계자(예: 프로젝트 관리자, 프로듀서, 편집장, 사고 대응 팀 등)에게 직접 상달 내용을 통보하도록 경보를 구성한다. | * 통보 시 보안 팀으로부터 적시의 대응이 없는 경우 이행할 수 있는 단계 확대 절차를 수립 및 구현한다. * 침범에 대해 사법당국에 자동 통보를 시행하는 것을 고려한다. * 주말 및 업무 외 시간 중의 통보 절차를 구현한다. |
| PS-5.4 | 경보 시스템 접근이 필요한 각 개인에게 고유의 작동 및 해제 코드를 할당하고 기타 모든 직원의 접근을 제한한다. | * 경보 작동/해제를 담당했던 보안 직원을 추적할 수 있도록 고유한 경보 코드를 사용한다. * 코드 공유 및 손실에 대한 위험을 줄일 수 있도록 할당된 경보 코드를 운영진이 승인한 주기마다 업데이트한다. |
| PS-5.5 | 시스템을 작동 및 해제할 수 있는 사용자의 목록을 분기마다 또는 담당자가 변경될 때마다 검토한다. | * 회사를 퇴직했거나 직무 역할이 변경된 사용자를 목록에서 삭제한다. * 삭제된 사용자에게 할당되었던 경보 코드를 비활성화한다. |
| PS-5.6 | 경보 시스템을 분기마다 테스트한다. | * 물리적 보안 침입을 모의실험하여 다음 사항을 확보한다. * 경보 시스템이 침입을 탐지함 * 보안 담당자가 통보를 받음 * 보안 담당자가 절차에 따라 적시에 대응함 |
| PS-5.7 | 정전, 방화문 미작동 및 무단 접근을 막기 위해 기타 모든 장치가 차단되지 않는 경우를 대비한 화재 안전 조치를 구현한다. |  |
| PS-6.0 | 권한 부여 | 시설 접근을 관리하는 절차를 문서화 및 구현하고 **접근 권한**의 변경 사항을 기록해둔다. | * 시설 접근을 허가할 담당자를 지명한다. * 직원 지위의 변경 사항을 관련 담당자(예: 시설 운영진)에게 통보한다. * **회사 관계자** 및/또는 **제3자 근무자**의 시설 접근을 요청할 때 상관이 작성해야 하는 서면 또는 전자식 양식을 마련한다. * 접근 요청의 조사 및 승인에 대한 책임을 할당한다. |
| PS-6.1 | 제작 시스템은 권한 있는 관계자만 접근할 수 있게 제한한다. |  |
| PS-6.2 | 제한 구역(예: **금고실**, 서버/장비실)의 출입을 분기별로 검토하고 **회사 관계자** 및/또는 **제3자 근무자**의 역할이나 고용 상태가 변경된 경우에도 검토한다. | * 해당 출입이 각 사용자에게 할당된 직무에 적절한지 확인한다. * 고용이 종료된 사용자의 접근 권한을 제거한다. * 접근이 사용자에게 할당된 직무에 적합한지 확인한다. |
| PS-7.0 | 전자식 출입 제어 | 모든 출입 지점과 콘텐츠가 보관, 운송 또는 처리되는 모든 구역을 커버하도록 시설 전체에 전자식 출입 시스템을 구현한다. | * 직무와 책임 사항을 바탕으로 특정 시설 구역에 대한 전자식 출입 권한을 할당한다. * 회사 관계자 및 제3자 근무자의 역할이 바뀌거나 고용이 종료되면 그에 따라 전자식 출입 권한을 업데이트한다. * 회사 관계자에게 전자식 출입 장치 번호를 할당한 로그를 기록한다. * 로깅 및 모니터링 PS-10.0을 참조한다. * 공동 구역(예: 공용 승강기)에 대한 전자식 출입이 필요하지 않은 시간대를 검토한다. |
| PS-7.1 | 전자식 출입 제어 | 전자식 출입 시스템의 관리를 적절한 관계자로만 제한한다. | * 전자식 시스템 관리를 지정된 담당자로만 제한하고 제작 콘텐츠에 접근하는 자가 전자식 출입에 대한 관리 작업을 수행할 수 없도록 한다. * 독자적 팀을 배정하여 전자식 출입을 시행, 관리하게 한다. |
| PS-7.2 | 카드지와 **전자식 출입 장치**(예: 키 카드, 키 홀더)는 잠금 장치가 달린 캐비닛에 보관하고 개인에게 할당되기 전에는 **전자식 출입 장치**가 비활성 상태로 유지되도록 한다. 할당되지 않은 전자식 출입 장치(예: 키 카드, 키 홀더)는 잠금 장치가 달린 캐비닛에 보관하고 개인에게 할당되기 전에는 비활성 상태로 유지되도록 한다. | * 잠금 장치가 달린 캐비닛에는 **키 카드**/**전자식 출입 장치** 시스템 관리 팀만 접근하게 제한한다. * 자료를 처분할 때에는 서명을 요구한다. |
| PS-7.3 | 분실된 **전자식 출입** 장치(예: 키 카드, 키 홀더)는 새로운 **전자식 출입 장치**를 발급하기 전에 시스템에서 비활성화한다. | * **회사 관계자** 및 **제3자 근무자**가 분실된 **전자식 출입 장치**를 즉시 신고하도록 교육하여 시설 내 무단 출입을 방지한다. * 교체 **전자식 출입 장치**를 발급하기 전에 ID를 요구한다. |
| PS-7.4 | 승인된 기간을 바탕으로 만료일(예: 90일)이 설정된 제3자 **전자식 출입 장치**를 발급한다. | * **제3자** **전자식 출입 장치**는 **회사 관계자** 전자식 출입 장치와 쉽게 구별할 수 있도록 한다. * **전자식 출입 장치**의 만료일은 쉽게 눈에 띄도록 한다. * **제3자** 전자식 출입 장치는 알 필요가 있는 경우에 할당한다. |
| PS-8.0 | 열쇠 | **마스터 열쇠** 및/또는 제한 구역 열쇠는 권한 있는 관계자(예: 소유자, 시설 경영진)에게만 배포하는 것으로 제한한다. | * **마스터 열쇠**를 빌릴 수 있도록 허용된 **회사 관계자** 목록을 작성, 유지한다. * 해당 목록을 정기적으로 업데이트하여 **마스터 열쇠** 사용이 더 이상 필요하지 않은 **회사 관계자**를 목록에서 삭제한다. |
| PS-8.1 | **마스터 열쇠** 및/또는 제한 구역 열쇠의 배포를 추적 및 모니터링할 수 있는 대여/반환 절차를 구현한다. | * 기록을 유지하여 다음 정보를 추적한다. * **각 마스터 열쇠를 소유하고 있는** 회사 관계자 * 대여/반환 시간 * 대여 사유 * 정해진 기간 내에 **마스터 열쇠**를 반환하도록 요구하고 제 시간에 반환되지 않은 키의 소재를 파악한다. |
| PS-8.2 | 외부 출입 지점에 대해 특정 자물쇠 제조업체만 복제할 수 있는 열쇠를 사용한다. | * 다음 중 두 가지 이상의 조작을 방지할 수 있는 높은 보안 수준의 열쇠(실린더 자물쇠)를 사용한다. * 강제로 따기 * 주형 뜨기 * 열쇠 복제 * 구멍 뚫기 * 기타 형태의 강제 진입 |
| PS-8.3 | 시설 출입 지점을 포함하여 **마스터 열쇠** 및 제한 구역 열쇠의 재고를 분기마다 조사한다. | * 소재가 불분명한 (분실/도난) 열쇠를 파악 및 조사하여 대처한다. * 기록지를 검토하여 소재를 알 수 없는 열쇠를 누가 마지막으로 대여했는지 파악한다. * 제한 구역에 대한 **마스터 열쇠**나 열쇠가 분실된 후 소재 파악이 불가능한 경우 자물쇠를 바꾼다. |
| PS-8.4 | 고용이 종료된 직원/제3자 또는 접근 권한이 더 이상 필요 없는 사람의 모든 키를 회수한다. |  |
| PS-8.5 | 열쇠 | 마스터 또는 보조 마스터 열쇠를 분실하거나 잃어버린 경우 전자식 출입을 통제하거나 전체 시설의 열쇠를 다시 만든다. |  |
| PS-9.0 | 카메라 | 모든 시설 출입 지점과 제한 구역(예: 서버/장비실 등)을 녹화하는 **CCTV** 시스템을 설치한다. | * 카메라 케이블과 배선은 따로따로 보이지 않게 감추고 쉽게 닿을 수 없는 곳에 있어야 한다. * 시설은 건물에 설치된 CCTV로 충분하다고 추정하지 않는다. * 시설의 모든 입구에 카메라를 배치한다. * 카메라가 보관 구역과 **금고실**을 커버하도록 한다. |
| PS-9.1 | 감시 영상의 적절한 범위, 기능, 화질, 조명 상태 및 프레임률을 보장하기 위해 카메라 위치 설정 및 녹화 영상을 최소한 매일 검토한다. | * 카메라 위치 설정을 검토하여 모든 출입 지점과 기타 민감한 구역에 대한 시야를 가로막는 물체가 없도록 한다. * 어두운 구역의 카메라를 조정한다(예: 저조명 또는 적외선 카메라, 동작 감지 조명). * 감시 로그가 최소 90일 동안 보존되고 있는지 감시 로그를 검토한다. * 프레임률을 검토하여 활동이 녹화 필름에 적절히 촬영되도록 한다. * 재생 중인 콘텐츠가 촬영되지 않도록 카메라 위치를 설정한다. * 얼굴의 특징을 식별할 수 있는 충분한 해상도로 녹화한다. * 프레임률은 최소 7로 녹화한다. |
| PS-9.2 | **CCTV** **콘솔** 및 **CCTV** 장비(예: DVR)에 대한 물리적 및 논리적 접근은 시스템 관리/감시를 책임지는 관계자로만 제한한다. | * **CCTV** 장비를 안전한 출입 통제 구역(예: 컴퓨터실, 잠금 장치가 달린 보관함, 케이지)에 둔다. * 정기적으로 출입을 검토하여 적절한 관계자만 감시 장비에 접근하도록 한다. * IP 기반 **CCTV** 시스템의 웹 콘솔은 권한 있는 관계자만 접근하도록 하고 강력한 계정 관리 수단을 이행한다(예: 복잡한 비밀번호, 개별 사용자 로그인, 로깅 및 모니터링). |
| PS-9.3 | 카메라 | 카메라 영상에 정확한 날짜와 타임 스탬프가 포함되고 **CCTV** 감시 영상과 전자식 출입 기록을 최소 90일 또는 법이 허용하는 최대 기간 동안 안전한 장소에 보존하도록 한다. | * 테이프 또는 디스크에 녹화되는 카메라 필름용 물리 **매체**에 시간과 날짜를 새긴다. * 디지털 카메라 녹화 장비에 정확한 타임 스탬프가 유지되도록 한다. * 날짜와 타임 스탬프의 정확도를 최소한 매주 검토한다. * 출입 통제된 전화통신 보관함이나 컴퓨터실에 로그를 보관할 수도 있다. * 일일 로깅에 필요한 일반적 공간을 정하여 로그 크기가 최소 90일, 또는 법이 허용하는 최대 보존 기간 동안의 기록을 담을 만큼 충분하도록 확보한다. * 최초 제작 공개일까지 CCTV 감시 영상을 보존하는 것을 고려한다. |
| PS-9.4 | 운영 시간 동안 감시 영상을 모니터링하고 탐지된 보안 사고를 즉시 조사할 직원 또는 직원 그룹을 지정한다. | * 보안 사고를 처리하는 사고 대응 절차를 포함시킨다. * 접수 데스크 또는 IT 사무실에 감시 모니터 추가를 고려한다. |
| PS-10.0 | 로깅 및 모니터링 | 최소한 매주 제한 구역의 전자식 출입에 대한 수상한 사건을 기록 및 검토한다. | * 의심이 드는 사건을 식별하여 문서화한다. * 의심스러운 전자 접근이 감지되었을 때 적절한 보안 요원에게 실시간 경고를 전송하는 자동화 보고 프로세스 구현을 고려한다. * 로그는 최소한 1년 동안 보존한다. * 다음 사건을 기록, 검토한다. * 반복된 출입 시도 실패 * 비정상적 시간의 출입 * 여러 구역 출입문의 연속적 통과 |
| PS-10.1 | 로깅 및 모니터링 | 다음 영역은 최소한 매일 전자식 출입을 기록하고 검토한다.   * 사전 마스터링 * 서버/장비실 * 스크랩실 * 보안이 철저한 케이지 * 이례적으로 간주되는 사건을 식별하고 문서화한다. | * 수상한 전자식 출입 활동이 탐지된 경우, 적절한 보안 담당자에게 실시간으로 통보하는 자동 보고 절차의 이행을 고려한다. * 수상한 전자식 출입 활동이 탐지된 경우, 적절한 보안 담당자에게 실시간으로 통보하는 자동 보고 절차의 이행을 고려한다. |
| PS-10.2 | 수상한 전자식 출입 활동이 탐지된 경우 이를 조사한다. | * 비정상적인 전자식 출입 활동이 탐지된 순간 통보를 받아야 할 주요 연락 담당자를 식별하여 알린다. * 일차 연락 담당자가 사건 통보에 대해 적시에 응답하지 않을 경우 따라야 할 단계 상달 절차를 수립, 이행한다. |
| PS-10.3 | 확인된 모든 전자식 출입 사고를 항상 기록하고 후속 조치가 취해진 경우 이에 대한 기록을 포함시킨다. | * **사고 대응** 보고 양식을 활용하여 확인된 **키 카드/전자식 출입 장치** 사고를 문서화한다. * 최근의 모든 **키 카드/전자식 출입 장치** 사고를 정기적으로 검토하고 근본 원인을 분석하여 취약점과 적절한 시정 조치를 파악한다. |
| PS-11.0 | 검색 | 보안 요원이 사람, 가방, 포장 상자 및 개인 물품에서 고객 콘텐츠를 무작위로 수색할 수 있도록 현지 법으로 허용되는 정책을 수립한다. | * 모든 **회사 관계자** 및 **제3자 근무자**에게 수색 관련 정책을 알린다. * **회사 관계자** 및 **제3자 근무자**에 대한 수색을 정기적으로 실시하여 정책을 실증한다. |
| PS-11.1 | 검색 | 다음을 포함하여 시설의 모든 직원과 방문객들에게 적용되는 출구 수색 절차를 구현한다:   * 수색을 위해 모든 외투, 모자, 벨트의 탈의 * 주머니 속 모든 내용물 꺼내기 * 보안 요원의 감독 하에 자체 몸수색 실시 * 모든 가방의 철저한 검사 * 랩톱 내 CD/DVD 플레이어 검사 * 수색 대상자로부터 약 3인치 거리에서 휴대용 금속 탐지기로 스캔 | * 시설 내 반입이 제한된 물품(예: 카메라)이나 적절한 허가 없이 시설 밖으로 반출할 수 없는 필름 자료를 찾도록 보안 요원에게 지시한다. * 모든 회사 관계자 및 제3자 근무자에게 출구 수색 관련 정책을 알린다. * 교대 근무를 통해 긴 행렬 및 장시간 대기를 방지한다. |
| PS-11.2 | 관계자가 디지털 기록 장치(예: **소형 USB** 드라이브, 디지털 카메라, 휴대폰)를 가지고 출입하는 것을 금지하고 이러한 장치의 수색을 기존 수색 절차의 일부로 포함시킨다. | * 발견된 모든 디지털 기록 장치를 압수하여 안전 로커에 보관한다. * 모든 콘텐츠 도난 시도 사고를 문서화한다. * 콘텐츠 도난을 시도한 당사자에 대해 필요한 징계 조치를 취한다. * 디지털 기록 기능이 내장된 이동식/휴대전화 장치를 금지하는 정책을 마련하고 의무 시행한다. * 개봉 흔적이 남는 스티커가 사용된 경우 디지털 기록 기능이 있는 휴대전화 사용을 허용한다. |
| PS-11.3 | 제작 구역으로 음식물을 반입할 때는 투명한 비닐 봉지와 식료품 용기를 사용할 것을 의무 시행한다. | * X |
| PS-11.4 | 너무 큰 의복(예: 배기 팬츠, 오버사이즈 후드 스웨터)의 착용을 금지하는 복장 규정 정책을 구현한다. |  |
| PS-11.5 | 시설로 반입/반출이 가능한 승인된 장치를 식별하기 위해 숫자로 된 개봉 흔적이 남는 투명 스티커/홀로그램을 사용한다. |  |
| PS-11.6 | 검색 | 출구 수색 절차를 시험하는 절차를 마련한다. | * 보안 요원이 철저한 수색을 할 수 있도록 수색 절차에 대한 주기적 감사를 수행한다. * 출구 수색 절차를 개선하는 방법을 파악한다. * 수색 절차의 모든 감사 결과 및 개선 내용을 문서화한다. |
| PS-11.7 | 시설에 주차장이 있는 경우 무작위 차량 수색 절차를 수행한다. |  |
| PS-11.8 | 매우 민감한 콘텐츠를 처리하는 복사 라인을 분리하고 기존 분리된 영역을 수색한다. |  |
| PS-11.9 | 보안 요원 활동을 모니터링하는 추가 관리 수단을 구현한다. | * 출구에서 보안 요원의 출구 수색 절차를 검토한다. * 보안 요원의 설비/제작 구역 감독 책임과 출구 지점에 대한 보안 요원의 책임(예: 수색 절차)을 분리한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| PS-12.0 | 인벤토리 추적 | 콘텐츠 자산 관리 시스템을 구현하여 물리적 자산(예: 고객이 시설에서 생성하여 수취된)을 상세히 추적한다. | * 공개 양식이나 작업 지시서를 요구하여 특정 개인이 콘텐츠를 대여할 수 있음을 확인한다. * 인증을 위해 신분증을 제시하도록 개인에게 요구한다. * 모든 자산에 태그(예: 바코드, 고유 ID)를 의무화한다. * 대여/반납된 모든 자산을 기록한다. * 각 자산의 예상 대여 기간을 기록한다. * 업무 시간이 끝나기 전까지 또는 승인된 기간 동안 반환되지 않은 자산을 통보하는 자동 경고 기능의 사용을 고려한다. * 대여 자산을 반환하지 않은 개인을 추적하여 후속 조치를 취한다. * 각 자산의 소재를 기록한다. * 각 집행의 시간과 날짜를 기록한다. |
| PS-12.1 | 고객 자산 및 생성된 매체(예: 테이프, 하드 드라이브)는 수취 시 바코드를 부착하거나 고유한 추적 ID를 할당하고 사용하지 않는 자산은 금고실에 보관한다. | * 이중 바코드를 적용하여 자산을 추적한다(즉, 자산 및 해당 컨테이너/상자 둘 다에 바코드 부착). * 바코드를 부착한 자산은 **금고실**로 바로 보내고 더 이상 필요하지 않은 자산은 **금고실**로 즉시 반환한다. |
| PS-12.2 | 자산 이동 집행 로그는 최소한 1년 동안 보존한다. | * 모든 자산 이동에 대한 물리적 또는 디지털 로그를 작성, 보관한다. 로그에는 다음이 포함되어야 한다. * 대여/반납된 자산의 바코드 또는 고유 ID * 대여/반납 시간과 날짜 * 자산을 대여한 개인의 이름과 고유 ID * 대여 사유 * 자산의 소재 |
| PS-12.3 | 인벤토리 추적 | 콘텐츠 **자산 관리** 시스템의 로그를 최소한 매주 검토하고 이례 사항을 조사한다. | * 예상 반환일까지 반환되지 않은 자산을 파악한다. * 소재를 알 수 없는 자산을 마지막으로 대여한 사람에 대해 후속 조사한다. * **자산 관리** 정책을 준수하지 않는 자에 대해 징계 절차를 이행한다. * 장기간 대여되는 자산에 대해 자동 통보를 구현할 것을 고려한다. |
| PS-12.4 | 가능한 경우 물리적 자산과 자산 추적 시스템에 스튜디오 필름 제목 별칭을 사용한다. | * 적절한 경우 물리적 자산에 표시된 스튜디오 이름을 삭제하는 것을 고려한다. |
| PS-12.5 | **금고실**로부터 대여되었으나 아직 반환되지 않은 매우 민감한 자산을 식별하기 위해 일별 미반환 경과 보고서를 작성 및 검토한다. | * 일별 미반환 경과 보고서를 직접 작성하거나 **자산 관리** 시스템을 통해 수행한다. * 모든 예외 사항을 조사한다. |
| PS-12.6 | 운송이 시간에 맞추어 전달되지 않는 경우, 지연되거나 반환되는 자산을 락업(lock up) 처리하고 기록한다. | * 접근 통제 영역에 자산을 보관하기 위한 절차를 정립한다. * 자산의 현장 보관을 기록하는 문서를 유지하고, 보관 날짜 및 사유를 기록에 포함시킨다. |
| PS-13.0 | 재고 합계 | 각 고객의 재고 개수를 분기마다 조사하고 **자산 관리** 기록과 대조하여 조정한 다음 부족분을 고객들에게 즉시 알린다. |  |
| PS-13.1 | **금고실** 직원과 재고 개수 조사를 책임지는 담당자의 업무를 분장한다. | * 비 **금고실** 담당 직원을 배정하여 개수 조사의 결과를 임의 확인케 한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| PS-14.0 | 공백 매체/생필름 추적 | 공백 매체/생필름은 수취 시 단위 별로 태그(예: 바코드, 고유 ID 할당)를 부착한다. | * 공백 또는 생 **매체**는 제작에 필요한 경우가 아니면 보안이 유지되는 제작 구역으적로 들여놓지 않는다. |
| PS-14.1 | 생 매체(예: 폴리카보네이트)의 소비량을 매달 추적하는 절차를 수립한다. | * 초과 시 사고 대응 절차를 가동하는 변동 임계값을 설정한다. * 초과 시 **사고 대응** 절차를 가동시키는 변동 임계값을 설정한다. * 월별 추적 절차의 일부로 생필름의 물리적 개수를 파악한다. |
| PS-14.2 | 공백 **매체**/생필름은 안전한 장소에 보관한다. | * 출입 통제수단(예: 잠금 장치가 달린 캐비닛, 금고)을 요구하여 무단 접근을 방지한다. * 공백 **매체**/생필름은 출력물 생성을 책임지는 담당자만 다루도록 제한한다. * 공백 **매체**/생필름 대여를 요청하는 적절한 작업주문 요청을 제시하도록 개인에게 요구한다. |
| PS-15.0 | 고객 자산 | 완성된 고객 자산은 자산 추적 및 관리를 책임지는 담당자만 접근하도록 제한한다. | * **금고실** 관리 팀만 접근하도록 제한한다. 금고실 관리 팀은 개인이 유효한 작업주문 요청을 제시한 경우 고객 자산을 대여하도록 허가할 수 있다. * 업무를 분장하여 **금고실** 관리 팀원이 제작 데이터의 처리를 취급하지 않도록 한다. |
| PS-15.1 | 고객 자산은 안전한 제한 구역(예: **금고실**, 금고 또는 기타 안전한 보관 위치)에 보관한다. | * 매우 민감한 제작물은 **금고실** 내 안전한 또는 보안이 철저한 케이지를 추가로 설치하여 보호한다. * 금고를 실내 구조에 볼트로 죄어 벽과 바닥에 고정시킨다. |
| PS-15.2 | 업무 시간 후 매우 민감한 구역(예: 금고, 보안 케이지)의 잠금은 두 명의 **회사 관계자**가 해제할 수 있도록 한다. |  |
| PS-15.3 | 고객 자산 | 배달되지 않은 소포를 시설에 밤새 보관할 때는 잠금 장치가 달린 내화성 금고를 사용한다. | * 움직일 수 없는 표면(예: 바닥, 벽)에 볼트를 사용하여 금고를 고정시킨다. |
| PS-15.4 | 잠금 장치로 잠그고, 출입을 통제하고, 감시 카메라 및/또는 보안 요원으로 감시하는 배달되지 않은 스크리너는 전용 보안 구역(예: 보안 케이지, 보안실)에 보관한다. | * 직무 수행을 위해 접근 필요한 사람으로 접근을 제한한다. * 스크리너 보관 구역은 완전한 봉쇄, 잠금 상태를 유지하여 항상 감시되도록 한다. * 감시 필름을 정기적으로 검토하는 절차를 이행한다. |
| PS-16.0 | 처분 | 고객 자산을 포함하는 거절되고, 손상되고, 더 이상 쓸모없는 재고는 처분하기 전에 삭제, 소자, 파쇄, 물리적으로 파기되어야 한다. | * 재고 조사 및 조정을 위한 절차를 이행한 다음, 거부되고, 파손되었으며, 더 이상 쓸모없는 재고를 안전하게 재활용하거나 파기한다. * 매체는 스크랩 통에 넣기 전에 복원할 수 없을 정도로 손상시킨다. * 미국방부의 디지털 파쇄 및 영구 삭제 표준인 5220.22-M의 참조를 고려한다(부록 G 참조). |
| PS-16.1 | 재활용/파기용 요소는 안전한 장소/컨테이너에 보관하여 처분 전 자산의 복제 및 재사용을 방지한다. | * 거부되고, 파손되었으며, 더 이상 쓸모없는 재고를 재활용/파기하기 전까지 보관하는 기간(예: 30일)을 제한하는 정책을 수립, 이행한다. * 매우 민감한 자산은 재활용/파기 전에 안전한 구역(예: **금고실**, 금고)에 보관한다. * 처분함은 잠가둔다. |
| PS-16.2 | 자산 처분 로그는 최소한 12개월 간 유지관리한다. | * 자산 처분 로깅은 **자산 관리** 절차와 통합한다. * 처분 로그에 처분된 자산의 최종 처분 기록을 포함시킨다. |
| PS-16.3 | 처분 | 파기는 현장에서 수행되어야 한다. 현장 파기는 두 명의 회사 관계자에 의해 감독되고 서명이 이루어져야 한다. 제3자 파기 회사를 고용하는 경우, 두 명의 회사 관계자가 파기를 감독하고 서명해야 하며 파기 자격증을 보유하고 있어야 한다. | * 파기 인증서에 다음 정보의 포함을 의무화하는 것을 고려한다. * 파기 날짜 * 파기/처분된 자산에 대한 설명 * 파기 방법 * 자산 파기 담당자 이름 |
| PS-16.4 | 거절된 디스크를 복사 장비에서 스크랩 통으로 직접 전달하는 자동화(장비 운전자 작업 불필요)를 실시한다. | * 처분 자동화가 가능하지 않은 경우 업무 분장을 실시한다(예: 검사 디스크를 만드는 담당자와 디스크를 파기하는 담당자를 분리함). * 디스크를 처분한 날짜와 시간을 서명 로그를 서명과 함께 유지한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| PS-17.0 | 운송 | 시설이 시설 외부로 고객 자산의 배송을 허가하는 유효한 작업/운송 지시서를 발행하도록 요구한다. | * 작업/운송 지시서에 다음 정보를 포함시킨다. * 작업/운송 지시 번호 * 콘텐츠를 집배할 담당자 이름과 소속 업체 * 취급 콘텐츠 * 시설 연락처 * 자산을 운반하기 전에 적절한 담당자의 허가를 받도록 요구한다 |
| PS-17.1 | 자산 운송 세부사항을 추적 및 기록하고 최소한 다음 사항을 포함시킨다.   * 배송 시간 * 발송인 이름 및 서명 * 수취인 이름 * 도착지 주소 * 배송업체가 발행한 추적 번호 * 해당 작업 지시서에 대한 참조 | * 수취인 서명을 요구한다 * 운송 로그는 최소 1년 동안 보존한다 |
| PS-17.2 | 집배 대기 중인 고객 자산을 보호한다. | * 경비인이 없을 때에는 운송 및 수취 구역의 모든 출입문과 창문을 잠근다. * 자산은 공급업체/배송업체로 인도되기 전까지 락업 상태여야 한다. |
| PS-17.3 | 시설을 떠나는 고객 자산을 유효한 작업/운송 지시서와 대조하여 확인한다. | * 배송물을 집배하는 담당자를 해당 작업 지시서와 대조하여 인증할 수 있도록 특송 및 배달 담당자로부터 유효한 신분증을 요구한다. * 발송 합계가 운송 서류상 정보와 일치하는지 확인한다. * 운송된 물품에 대한 불일치 또는 손상을 즉시 보고한다. |
| PS-17.4 | 운송 | 특송 및 배달 담당자가 시설 내 콘텐츠/제작 구역에 들어가도록 허용하지 않는다. | * 콘텐츠/제작 구역의 출입이 필요한 경우, 배달 담당자와 동행한다. |
| PS-17.5 | 트럭 운전사 정보에 대한 별도의 로그를 문서화하고 유지한다. | * 모든 트럭 운전사의 로그를 유지하고 다음 정보를 포함시킨다. * 이름 * 트랙터 및 트레일러의 번호판 * 제휴회사 * 집배 시간과 날짜 * 취급 콘텐츠 |
| PS-17.6 | 운송 전에 트레일러의 현장 적재 및 봉인을 관찰하고 감시한다. | * 트레일러의 적재 및 봉인 시 보안 요원이 항시 동행한다. |
| PS-17.7 | 시설 간 운송에 필요한 이동 시간, 경로 및 배송 시간을 기록, 모니터링 및 검토한다. | * 큰 오차는 조사, 보고하고 적절한 관계자에게 상달한다. * 주요 변동 사항을 조사, 보고 및 적절한 담당자에게 승계한다. * 허가 휴게소를 지정한다. * 예상치 못한 지연을 모니터링하고 경보하는 실시간 GPS 추적 시스템의 구현을 고려한다. |
| PS-17.8 | 고객 스튜디오의 승인된 목적 이외로 필름 요소의 전달을 금지한다. |  |
| PS-17.9 | 극장 개봉 전 심사용 인쇄물은 나누어서(예: 홀수 vs. 짝수 릴) 운송한다. |  |
| PS-18.0 | 수취 | 배달된 고객 자산은 수취 시 검사하고 운송 서류(예: 물품 명세서, 적하 목록)와 비교한다. | * 불일치 사항(예: 누락된 물품, 파손된 **매체**)을 파악, 기록한다. * 운영진, 고객 및/또는 발송인에게 불일치 사항을 즉시 보고한다. |
| PS-18.1 | 수취 | 배달물 수취 시 지정된 담당자가 작성하는 수취 기록지를 유지관리한다. | * 다음 정보를 기록한다. * 특송/배달 업체의 이름과 서명 * 수취인 이름과 서명 * 수취 시간과 날짜 * 수취한 자산의 세부사항 |
| PS-18.2 | 다음 작업을 즉시 수행한다.   * 수취한 자산에 태그(예: 바코드, 고유 ID 할당) 부착 * **자산 관리** 시스템에 자산 입력 * 제한 구역(예: **금고실**, 금고)으로 자산 이전 | * 즉시 태그를 부착하여 금고실로 이전할 수 없는 수취 자산은 안전한 **중간대기 구역**(예: 보안이 철저한 케이지)에 보관한다. |
| PS-18.3 | 야간 배달물 수취에 대한 안전한 방법을 구현한다. | * 수취 예상 물품에 대한 일정은 알 필요가 있는 관계자만 볼 수 있도록 한다. |
| PS-19.0 | 라벨 부착 | 고객이 달리 지시한 경우를 제외1하고 소포 바깥에 별칭(“별칭”)을 포함한 제작물 정보의 표기를 금지한다. |  |
| PS-20.0 | 포장 | 모든 고객 자산은 폐쇄/봉인된 컨테이너로 배송하고 자산 가치에 따라 또는 고객의 지시가 있는 경우 잠금 장치가 달린 컨테이너를 사용한다. |  |
| PS-20.1 | 다음 관리수단 중 하나 이상을 이행한다.   * 개봉 흔적이 남는 봉인 테이프 * 개봉 흔적이 남는 포장 * 개봉 흔적이 남는 밀봉재(예: 홀로그램 형태) * 안전한 컨테이너(예: 부호 자물쇠가 달린 펠리컨 케이스) | * 개봉된 흔적이 있는 상품을 처리하는 방법에 대한 계획을 수립하고 알린다 * 모든 개봉 사건은 사고 대응 팀으로 보고한다(MS-5.0) |
| PS-20.2 | 포장 | 모든 화물에 수축 포장을 하고 최종 배송 전에 포장이 적절한지 포장 상태를 검사한다. | * 개별 자산에 수축 포장을 하거나(예: 스키드, 팔레트) 대량 운송의 경우에는 스핀들에 따라 적용한다. |
| PS-21.0 | 운송 차량 | 차량과 트럭은 항상 잠그고 눈에 띄는 곳에 소포를 두지 않는다. | * 소포는 사람이 없는 곳에 방치하지 않는다. |
| PS-21.1 | 운송 차량(예: 트레일러)에 다음의 보안 기능을 포함시킨다.   * 운전실과 분리 * 화물칸 문을 잠그고 봉인할 수 있는 기능 * 엄격한 보안이 필요한 운송품에 대한 GPS | * 민감한 콘텐츠 및 고가의 자산을 배송할 때는 GPS 추적 시스템이 장착된 차량을 사용한다. |
| PS-21.2 | 매우 민감한 제작물을 배송할 때는 화물칸 도어에 볼트형 봉인을 사용한다. | * 보안 요원이 밀봉을 적용, 기록 및 모니터링한다. * 매우 민감한 소포에는 추가 보안 조치를 고려한다(예: 잠금/보안이 작동하는 화물칸, 잠금 장치가 달린 펠리컨 케이스). |
| PS-21.3 | 고위험 구역에 매우 민감한 콘텐츠를 배송할 때는 보안 경호를 이용하도록 한다. | * 강탈, 강도 및 콘텐츠 도난을 초래할 수 있는 그 밖의 시나리오로부터 매우 중요한 콘텐츠를 보호할 수 있는 보안 요원을 고용한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| DS-1.0 | 방화벽/WAN/  경계 보안 | 내부 네트워크로 무단 접근을 차단하고 업로드 및 다운로드 트래픽을 동일하게 유지할 수 있는 접근제한목록(ACL)이 있는 검사 방화벽을 사용하여 외부 네트워크/WAN을 내부 네트워크와 분리한다. | * **DMZ**에 상주하는 명시적 호스트를 제외한 내부 네트워크로의 모든 트래픽을 거부하는 접근제한목록이 포함된 **WAN** **방화벽**을 구성한다. * 내부 콘텐츠/제작 네트워크에 대한 직접적인 네트워크 접근을 금지하도록 **WAN** 네트워크를 구성한다. * 모든 외부 연결 장치와의 연결 수를 정확하게 보여주고 설명하는 상세한 WAN 문서를 포함한다. * 방화벽 규칙은 모든 트래픽 및 모든 구성 변경에 대한 로그를 생성하도록 구성되어야 하며 로그는 최소한 매월 검사해야 한다. * 방화벽은 바이러스 백신 및 침입 탐지 업데이트가 자동으로 되어야 하며 업데이트는 최소한 매주마다 이루어져야 한다. * 방화벽 구성에 다음을 포함할 것을 고려한다. * 안티 스푸핑 필터 * 라우팅되지 않는 IP 주소 차단 * 외부 포트에서 내부 주소 차단 * UDP 및 ICMP 에코 요청 차단 * 미사용 포트 및 서비스 차단 * 미승인 DNS 영역 전송 차단 * 나가는 트래픽이 내부 주소에서 들어올 수 있도록 출구 필터 적용 |

|  |  |  |  |
| --- | --- | --- | --- |
| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| DS-1.1 | 방화벽/WAN/  경계 보안 | 방화벽 접근제한목록(**ACL**)을 검토하는 절차를 수립하여 6개월마다 구성 설정의 적절성과 업무상 필요성을 확인한다. | * 방화벽 및/또는 라우터의 **ACL**을 내보내기한다. * **ACL**을 검토하여 네트워크 접근이 적절한지 확인한다. * 경영진이 검토 내용 및 방화벽 규칙 변경에 서명하도록 한다. * **ACL**을 적절하게 업데이트한다. |
| DS-1.2 | 기본 설정으로 WAN과 방화벽에 접근하는 모든 프로토콜을 거부하고 허용된 특정 보안 프로토콜만 활성화한다. | * **텔넷** 및 **FTP** 등의 암호화되지 않은 모든 통신 프로토콜을 제한한다. * 비암호화 프로토콜은 암호화 프로토콜로 대체한다. |
| DS-1.3 | 외부에서 접근 가능한 서버(예: 웹 서버)는 **DMZ** 내에 둔다. | * **DMZ** 내 서버를 분리하여 서버(예: 웹 서버 등) 당 한 종류의 서비스만 제공하게 한다. * **ACL**을 구현하여 **DMZ**의 내부 망 접근을 제한한다. |
| DS-1.4 | 네트워크 인프라 장치(예: 방화벽, 라우터, 스위치 등), SAN/NAS(Storage Area Networks and Network Attached Storage, 저장 영역 네트워크 및 네트워크 부착 저장) 및 서버에 대한 패치 절차를 구현한다. | * 네트워크 인프라 장치, SAN/NAS 및 서버에 대한 패치를 정기적으로(예: 매월) 식별, 평가, 테스트하는 절차를 구현한다. * 심각한 보안 취약점을 다루는 패치 수준으로 네트워크 인프라 장치, SAN/NAS 및 서버를 업데이트한다. * 중요 패치는 48시간 내에 처리한다. * 중앙 관리식 패치 관리 시스템의 배포를 고려한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| DS-1.5 | 방화벽/WAN/  경계 보안 | 보안 구성 표준을 바탕으로 네트워크 인프라 장치, SAN/NAS 및 서버를 강화한다. SNMP를 사용하지 않거나 SNMPv3 이상만 사용하는 경우, SNMP(Simple Network Management Protocol, 단순 네트워크 관리 프로토콜)를 비활성화하고 강력한 비밀번호인 SNMP 커뮤니티 문자열을 선택한다. | * 다음 강화 옵션을 고려한다. * 게스트 계정 및 공유 비활성화 * 바이러스 백신/멀웨어 방지 프로그램 설치 * 소프트웨어 방화벽 활성화 * 불필요한 소프트웨어 제거 * 불필요한 서비스 설치 제거/비활성화 * 모든 사용자를 제한 사용자로 요구 * SNMP를 사용한 연결에 승인된 관리 시스템만 사용할 수 있도록 장치에 대한 접근을 제한하는 **ACL**을 사용한다. * 네트워크 인프라 장치를 강화하는 방법은 다음 보안 강화 표준을 참조한다. * NIST * SANS * NSA |
| DS-1.6 | 외부 인터페이스에서 방화벽을 원격으로 관리할 수 없도록 한다. | * 대신 2단계 인증과 **VPN**을 128비트 이상의 고급 암호화 표준(AES)과 함께 사용하여 원격 관리 기능을 수행한다. * 관리자 이외의 원격 접근 시 다음 중 2개를 제공하도록 요구한다. * 개인이 알고 있는 정보(예: 사용자 이름, 비밀번호) * 개인이 가지고 있는 고유한 실제 물건(예: 토큰, **키 카드**, 스마트폰, 인증서) * 개인에게 고유한 신체/생체인식 특성(예: 지문, 망막) |
| DS-1.7 | 방화벽/WAN/  경계 보안 | 네트워크 인프라 장치, SAN/NAS 장치 및 서버의 백업은 내부 네트워크 상의 중앙 보안 서버에 저장한다. | * 구성 파일 백업을 내부 네트워크 상에 안전하게(예: 암호화하여) 저장하도록 네트워크 인프라 장치를 구성한다. * 권한 있는 관리자만 저장 위치 및 암호화된 백업에 접근하도록 한다. * 백업에 비연결형 파일 전송 프로토콜(TFTP, Trivial File Transfer Protocol)을 사용하는 경우, 무차별 공격 및 구성 파일에 대한 무단 접근을 억제하는 제한을 설정한다. |
| DS-1.8 | 모든 외부 IP 범위와 호스트에 최소한 분기마다 취약성 검사를 수행하고 문제를 수정한다. | * 콘텐츠에 무단 접근할 수 있는 중요한 문제를 적시에 수정한다. * 가상화 기술을 사용하는 경우, 이 기술을 검사/테스트하는 도구가 포함되어 있는지 확인한다. * 독립된 제3자가 이를 수행하는 것을 고려한다. |
| DS-1.9 | 모든 외부 IP 범위와 호스트에 최소한 1년에 한 번 침투 테스트를 수행하고 문제를 수정한다. | * 콘텐츠에 무단 접근할 수 있는 중요한 문제를 적시에 수정한다. * 가상화 기술을 사용하는 경우, 이 기술을 검사/테스트하는 도구가 포함되어 있는지 확인한다. * 독립된 제3자가 이를 수행하는 것을 고려한다. |
| DS-1.10 | 전용 개인 연결을 사용하고 암호화를 사용하여 지점 간 연결을 보호한다. | * 암호화에는 128비트 이상의 고급 암호화 표준(AES)을 사용한다. |
| DS-1.11 | 모든 시스템이 공통 시간을 참조하도록 동기화된 시간 서비스 프로토콜(예: NTP(Network Time Protocol, 네트워크 시간 프로토콜))을 구현한다. | * 시스템의 시간이 정확하고 일정하도록 한다. * 시간 데이터가 보호되도록 한다. * 시간 설정이 산업 승인 시간 원본에서 수신되도록 한다. |
| DS-1.12 | 방화벽/WAN/  경계 보안 | WAN 네트워크 인프라 장치 및 서비스에 대한 기본 보안 요구사항을 수립, 문서화 및 구현한다. | * 취약성을 만들 수 있는 시스템 기본값이 생산에 들어가기 전에 수정되도록 한다. * 보안 기준에 반하여 인프라의 보고 규정준수를 지속적으로 모니터링하는 것을 고려한다. |
| DS-2.0 | 인터넷 | 디지털 콘텐츠를 처리하거나 저장하는 제작 네트워크 및 모든 시스템이 이메일을 포함하여 인터넷에 직접 접근하는 것을 금지한다. 제작 네트워크에서 또는 디지털 콘텐츠를 처리하거나 저장하는 시스템에서 인터넷 접근이 필요한 경우, 원격 호스팅 응용 프로그램/데스크톱 세션을 사용하는 승인된 방법만 허용된다. | * 인터넷 게이트웨이 시스템(예: Citrix, Terminal Services, VNC 등)을 사용하는 예외 사항은 다음 관리 방안으로 처리한다. * 웹 검색이 서버의 유일한 기능이 되도록 시스템을 엄격히 통제한다. * 웹 기반 이메일 사이트, P2P, 디지털 사물함 및 알려진 기타 악성 사이트를 비롯한 규제 사이트의 접근을 금지한다. * 시스템과의 콘텐츠 송수신을 제한한다. * 시스템에 패치를 정기적으로 적용하고 최신 바이러스 백신으로 업데이트한다. * 시스템 활동을 정기적으로 검토한다. * 로컬 드라이브 연결을 차단하고, USB 대용량 기억 장치를 차단하고, 프린터 연결을 차단하고, 복사 및 붙여넣기 기능을 차단하고, 제작 네트워크에서 인터넷 게이트웨이 시스템으로 다운로드/업로드를 차단한다. * 모든 아웃바운드 트래픽을 기본적으로 거부하고, 바이러스 백신 정의 서버, 패치 서버, 라이선싱 서버(로컬 라이선스를 사용할 수 없는 경우에만)와 같은 지정된 내부 네트워크로의 아웃바운드 전송이 필요한 특정 시스템과 포트를 명시적으로 허용하는 **방화벽** **규칙**을 구현한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| DS-2.1 | 인터넷 | 이메일 필터링 소프트웨어 또는 **비제작 네트워크**에서 발신되는 다음 트래픽을 차단하는 어플라이언스를 구현한다.   * 잠재적인 피싱 이메일 * 금지된 첨부 파일(예: Visual Basic 스크립트, 실행 파일 등) * 최대 10MB의 파일 크기 제한 * 멀웨어 또는 바이러스의 근원인 알려진 도메인 | * 이메일 첨부 파일 및 이메일 본문으로 사용할 수 없도록 제한된 콘텐츠 종류를 식별한다. * 이메일 필터링 솔루션을 구현하고 제한된 콘텐츠 종류를 바탕으로 구성한다. |
| DS-2.2 | 웹 필터링 소프트웨어를 구현하거나 P2P 파일 거래, 바이러스, 해킹 또는 기타 악성 사이트로 알려진 웹사이트로의 접근을 제한하는 어플라이언스를 구현한다. | * 웹 필터링/프록시 서버 소프트웨어를 구현하여 악성 웹사이트에 대한 접근을 탐지 및 방지한다. |
| DS-3.0 | LAN/내부 네트워크 | **콘텐츠/제작 네트워크**와 **비제작 네트워크**(예: 사내망, **DMZ**, 인터넷 등)를 물리적 또는 논리적 망 구분으로 분리한다. | * 접근이 필요한 특정 호스트(예: 바이러스 백신 서버, 패치 관리 서버, 콘텐츠 전달 서버 등)에서 **콘텐츠/제작 네트워크**로 접근하는 것을 명시적으로 허용하는 접근제한목록(ACL)을 정의한다. * 접근을 허용해야 할 포트와 서비스를 명시적으로 정의하여 **접근제한목록**에 포함시킨다. * 정의된 보안 구역을 바탕으로 네트워크를 구분 또는 분리한다. * 모든 아웃바운드 트래픽을 기본적으로 거부하고, 바이러스 백신 정의 서버, 패치 서버, 콘텐츠 전달 서버, 라이선싱 서버(로컬 라이선스를 사용할 수 없는 경우에만)와 같은 지정된 내부 네트워크로의 아웃바운드 전송이 필요한 특정 시스템과 포트를 명시적으로 허용하는 **방화벽** **규칙**을 구현한다. * 모든 인바운드 트래픽을 기본적으로 거부하고, 지정된 콘텐츠 전달 서버로부터의 인바운드 전송을 필요로 하는 특정 시스템 및 포트를 명시적으로 허용하는 **방화벽 규칙**을 구현한다. * 제작 환경 상의 인터넷 접근에 대한 지침은 DS-2.0을 참조한다. * **스위치**의 MAC 주소로 **정적 IP** **주소**를 할당한다. * **콘텐츠/제작 네트워크**의 **DHCP**를 비활성화한다. * 제작 컴퓨터 시스템이 한 번에 하나 이상의 네트워크에 연결하는 것을 금지한다. * 콘텐츠가 비제작 네트워크에서 사용되거나 저장되는 것을 금지한다. |
| DS-3.1 | 콘텐츠/제작 시스템은 권한 있는 관계자만 접근할 수 있게 제한한다. | * 네트워크 케이블을 대체/비승인 장치에 연결할 수 없도록 물리적 이더넷 케이블 잠금 장치의 사용을 고려한다. |
| DS-3.2 | LAN/내부 네트워크 | 직무를 수행하기 위해 접근이 필요한 승인된 관계자만 **콘텐츠/제작 네트워크**를 원격 접근할 수 있도록 제한한다. | * 콘텐츠/제작 네트워크에 원격으로 접근하는 것을 금지한다. * **콘텐츠/제작 네트워크**의 원격 접근이 허용된 **회사 관계자** 목록을 유지, 관리한다. * **콘텐츠/제작 네트워크**에 상주하는 시스템에 대한 접근을 모니터링하여 원격 활동을 검토하기 위한 관리 절차를 개발한다. * 원격 접근 시스템이 개별 계정을 사용하도록 구성한다. * 원격 접근은 접근제한목록을 통한 단일 방법으로 제한한다. * 비상 원격 접근이 필요한 경우에 대비해 다음을 구현한다. * 2단계 인증을 사용하고 인증서 기반을 지향한다. * FTP, SSH, IRC, IM을 포함하는 파일 전송 프로토콜을 차단한다. * **VPN** 구성은 분할 터널링을 허용하지 않아야 한다. * 제작 네트워크에 연결할 중간 단계로 런치패드/방어용 호스트 모델을 활용한다. |
| DS-3.3 | 스위치/계층 3 장치를 사용하여 네트워크 트래픽을 관리하고 **콘텐츠/제작 네트워크**에서 사용되지 않는 모든 **스위치** 포트를 비활성화하여 미승인 장치에 의한 패킷 스니핑을 방지한다. | * 장치 관리자가 다음과 같은 강력한 인증 방법을 사용하도록 요구한다. * 암호화된 프로토콜 * 비밀번호에 대한 솔티드 해시(Salted hash) * 실행 명령에 대한 개별 비밀번호 * 장치 콘솔에 접속하여 미사용 **스위치** 포트를 비활성화하도록 구성 파일을 업데이트한다. * 스위치/계층 3 장치에 대한 로깅을 활성화한다. |
| DS-3.4 | **콘텐츠/제작 네트워크**에서 허브 및 중계기 등의 비교환 장치 사용을 제한한다. | * 모든 허브/중계기를 **스위치** 또는 계층 3 장치로 교체한다. |
| DS-3.5 | LAN/내부 네트워크 | **콘텐츠/제작 네트워크** 내에 있는 컴퓨터 시스템의 이중 홈 방식 네트워킹(물리적 네트워크 브리징)을 금지한다. | * 대신 한 컴퓨터 시스템에 다중 NIC를 사용하는 대신 네트워크 계층(예: **라우터**, **방화벽**, **스위치** 등)에 논리적 네트워크 브리징을 사용한다. |
| DS-3.6 | **콘텐츠/제작 네트워크**에 네트워크 기반 침입 탐지/방지 시스템(**IDS/IPS**)을 구현한다. | * 수상한 네트워크 활동에 대해 경고하거나 이를 방지하도록 네트워크 기반 침입 탐지/방지 시스템을 구성한다. * **IDS/IPS**용 바이러스 백신/멀웨어 방지 프로그램에 가입한다. * **IDS/IPS**에 대한 공격 시그니처 정의/정책 및 바이러스 백신/멀웨어 방지 프로그램을 최소한 주마다 업데이트한다. * **IDS/IPS**에 대한 모든 활동 및 구성 변경을 기록한다. * 모든 워크스테이션에 호스트 기반의 침입 탐지 시스템 소프트웨어를 구현한다. |
| DS-3.7 | SNMP를 사용하지 않거나 SNMPv3 이상만 사용하는 경우, SNMP를 비활성화하고 강력한 비밀번호인 SNMP 커뮤니티 문자열을 선택한다. | * SNMP를 사용한 연결에 승인된 관리 시스템만 사용할 수 있도록 장치에 대한 접근을 제한하는 **ACL**을 사용한다. |
| DS-3.8 | 시스템을 **LAN/내부 네트워크**에 배치하기 전에 강화한다. | * 제안 사항은 DS-1.5 참조 |
| DS-3.9 | 최소한 1년에 한 번 내부 네트워크 취약성 검사를 수행하고 문제를 수정한다. | * 가상화 기술을 사용하는 경우, 이 기술을 검사하는 도구가 포함되어 있는지 확인한다. * 다음을 포함한다. * 제작 네트워크 * 비제작 네트워크 * 연결된 장비/장치 * 연결되지 않은 장비/장치 |
| DS-3.10 | LAN/내부 네트워크 | LAN, SAN/NAS, 장치, 서버 및 워크스테이션의 백업은 내부 네트워크 상의 중앙 보안 서버에 저장한다. | * 구성 파일 백업을 내부 네트워크 상에 안전하게(예: 암호화하여) 저장하도록 LAN 장치를 구성한다. * 권한 있는 관리자만 저장 위치 및 암호화된 백업에 접근하도록 한다. |
| DS-4.0 | 무선/WLAN | **콘텐츠/제작 네트워크**에서 무선 네트워크 연결 및 무선 장치 사용을 금지한다. | * 무선 게스트 네트워크가 인터넷만 접근하도록 하고 **콘텐츠/제작 네트워크**로의 접근은 제한한다. * 콘텐츠/제작 네트워크에서 콘텐츠를 처리하거나 저장하는 워크스테이션/랩톱에 대한 무선 접근 권한을 제거하거나 비활성화한다. |
| DS-4.1 | 무선/WLAN | **비제작** 무선 네트워크(예: 관리자 및 게스트)를 다음과 같은 보안 관리수단으로 구성한다.   * WEP/WPA 비활성화 * **AES**128 **암호화(WPA2)** 이상만 활성화한다. * “게스트” 네트워크를 사내 타 네트워크와 분리 * 기본 관리자 로그인 자격 증명서 변경 * 기본 네트워크 이름(**SSID**) 변경 | * 다음과 같은 보안 관리수단을 고려한다. * 회사와 관련 없는 특정 **SSID** 이름 사용 * 옵션이 제공되는 경우 IEEE 802.1X 또는 IEEE 802.11i 사용 * 옵션이 제공되는 경우 인증에 RADIUS 사용 * **MAC 주소 필터링**을 사용한다. * 제작 워크스테이션 및 장치의 무선 MAC 주소를 블랙리스트에 추가한다. * 무선 접근점/컨트롤러가 요구된 범위 내에서만 브로드캐스트하도록 구성한다. * 무선 네트워크 연결을 위해 다음을 포함하는 802.1X 프레임워크를 구현한다. * 인증, 권한 부여 및 과금징수를 위한 RADIUS(Remote Authentication Dial In User Service) * 사용자 계정 관리를 위한 Active Directory 등의 LDAP(Lightweight Directory Access Protocol) 서버 * 클라이언트 및 서버 인증서 생성과 관리를 위한 공용 키 인프라 * 사전 공유된 키를 사용해야 하는 경우 다음 관리수단을 구현한다. * WPA2를 CCMP(**AES-128** 이상) **암호화**로 구성한다. * 복잡한 비밀문구를 설정한다(비밀문구 복잡성에 대한 권장 사항은 DS-8.1을 참조). * 비밀문구를 최소한 90일마다 변경하고 주요 **회사 관계자**의 고용이 종료될 때에도 변경한다. |
| DS-4.2 | 무선/WLAN | 비인증 무선 접근점을 검사하는 절차를 구현하고 확인된 문제를 수정한다. | * 최소한 분기마다 시설을 순찰하여 비보호된 무선 접근점을 검사하는 절차를 구현한다. * 가능한 경우, 집중화된 무선 접속 솔루션(즉, 무선 컨트롤러)이 비인증 무선 접근점을 탐지한 즉시 관리자에게 통보하도록 구성한다. |
| DS-5.0 | 입출력 장치 보안 | 콘텐츠 입출력(I/O)에 사용할 특정 시스템을 지정한다. | * 특정 발신/수신 **IP 주소**에 대해 **콘텐츠/제작 네트워크**와 입출력용 시스템 간의 트래픽을 허용하도록 **ACL**을 구현한다. |
| DS-5.1 | 콘텐츠를 처리하거나 저장하는 모든 시스템에서 입출력(I/O), 대용량 기억, 외부 저장 및 모바일 저장 장치(예: **USB**, **FireWire**, Thunderbolt, SATA, **SCSI** 등) 및 광학 매체 버너(예: DVD, Blu-Ray, CD)를 차단하고 콘텐츠 입출력에 사용되는 시스템은 예외로 한다. | * **입출력 장치** 차단에 다음을 고려한다. * MS Windows 기반 시스템의 경우 **입출력 장치**로의 쓰기 접근을 제한하도록 레지스트리 설정을 변경한다. * Mac 기반 시스템의 경우 대기억 파일을 삭제하여 제작 스테이션의 쓰기 접근을 제한한다. * Microsoft Active Directory 또는 Apple Open Directory를 사용하는 시스템의 경우 그룹 정책을 통해 **입출력 장치**를 비활성화한다. * 출력 장치 차단이 실행 불가능한 경우 입출력 포트 감시 소프트웨어를 사용하여 포트 사용을 탐지한다. |
| DS-6.0 | 시스템 보안 | SAN/NAS 시스템에 연결하는 모든 워크스테이션, 서버 및 장치에 바이러스 백신 및 멀웨어 방지 소프트웨어를 설치한다. | * 중앙 집중식 관리 콘솔이 포함된 기업용 바이러스 백신 및 멀웨어 방지 솔루션을 설치한다. * 종점 보호의 설치를 고려한다. |
| DS-6.1 | 모든 바이러스 백신 및 멀웨어 방지 정의를 매일 또는 더 자주 업데이트한다. | * 최소한 매일 중앙 집중식 바이러스 백신 및 멀웨어 방지 관리 콘솔이 정의 업데이트를 다운로드 및 푸시하도록 구성한다. |
| DS-6.2 | **콘텐츠/제작 네트워크**로 입력하기 전에 모든 콘텐츠에 대해 바이러스 및 멀웨어를 검사한다. | * **콘텐츠/제작 네트워크**로 연결되지 않은 시스템을 스캔한다. |
| DS-6.3 | 시스템 보안 | 다음과 같은 검사를 수행한다.   * 모든 워크스테이션에서 시스템 전체를 대상으로 하는 정기적인 바이러스 및 멀웨어 검사 활성화 * SAN/NAS에 연결된 서버 및 시스템에서 시스템 전체를 대상으로 바이러스 및 멀웨어 검사 활성화 | * 바이러스 백신 및 멀웨어 방지 소프트웨어가 바이러스 백신 및 멀웨어 방지 전략을 바탕으로 전체 시스템 검사를 실시하도록 구성한다. * 바이러스 백신 멀웨어 방지 소프트웨어가 유휴 시간 동안에 실행되도록 구성한다. |
| DS-6.4 | 보안 취약점을 수정하는 패치/업데이트로 시스템(예: 파일 전송 시스템, 운영체제, 데이터베이스, 응용 프로그램, 네트워크 장치)을 정기적으로 업데이트하는 절차를 구현한다. | * 가능한 경우 모든 시스템에 패치를 자동 배포할 수 있는 집중화된 패치 관리 도구(예: WSUS, Shavlik, Altiris)를 구현한다. * 공급업체 및 기타 제3자 업체로부터 패치를 구한다. * 배포 전에 패치를 시험한다. * 시스템 패치 미적용에 대해 정당한 업무 사례가 있는 경우 이에 대한 예외 절차 및 보완 관리수단을 구현한다. |
| DS-6.5 | 소프트웨어(예: ProTools, Clipster 그리고 Blu-Print, Scenarist 및 Toshiba와 같은 저작 소프트웨어)로 인해 필요한 경우를 제외하고, 사용자가 자체 워크스테이션에서 관리자가 되는 것을 금지한다. 소프트웨어 공급자의 문서에 관리자 권한이 필요하다는 명백한 설명이 있어야 한다. | * 워크스테이션에 로그인하는 데 사용되는 사용자 계정이 시스템 관리자 권한을 가지지 않도록 한다. |
| DS-6.6 | 콘텐츠를 처리하는 휴대용 컴퓨터 장치(예: 랩톱, 태블릿, 타워)가 사람 없이 방치될 경우 케이블 잠금 장치를 사용한다. | * 케이블 잠금 장치를 고정 물체(예: 탁자)에 고정한다. |
| DS-6.7 | 시스템 보안 | 고객 프로젝트와 관련된 콘텐츠 또는 민감한 정보가 포함된 랩톱 및 휴대용 컴퓨터 저장 장치에 대한 추가 보안 관리수단을 구현한다. 모든 랩톱을 암호화한다. 하드웨어를 암호화한 휴대용 컴퓨터 저장 장치를 사용한다. 하드 드라이브 및 기타 저장 장치의 원격 영구 삭제가 가능하도록 콘텐츠를 처리하는 모든 랩톱/모바일 장치에 원격 제거 소프트웨어를 설치한다. | * 랩톱을 안전하지 않은 장소에서 사용해야 하는 경우 사생활 보호 스크린을 부착한다. * 랩톱을 공공 무선 장소에 연결하지 않는다. * 사용하지 않을 때는 랩톱의 전원을 끄고 절전 또는 최대 절전 모드를 사용하지 않는다. |
| DS-6.8 | 소프트웨어 설치 권한을 IT 관리자로 제한한다. | * 비인증 소프트웨어(예: 불법 또는 악성 소프트웨어)를 포함한 미승인 소프트웨어의 설치와 사용을 금한다. * 최소한 분기마다 모든 시스템에서 설치된 응용 프로그램의 인벤토리를 검사한다. |
| DS-6.9 | 내부적으로 설치되는 시스템(예: 랩톱, 워크스테이션, 서버, SAN/NAS)의 구성을 위한 보안 기준 및 표준을 구현한다. | * 모든 시스템의 이미지를 만드는 데 사용되는 보안 표준 빌드를 개발한다. |
| DS-6.10 | 불필요한 서비스와 응용 프로그램은 콘텐츠 전송 서버에서 설치 제거되어야 한다. | * 모든 콘텐츠 전송 서버에 설치된 서비스(예: services. MSc) 목록을 검토하고 필요 없는 서비스를 설치 제거 또는 비활성화한다. * 모든 콘텐츠 전송 서버의 설치된 응용 프로그램 목록을 검토하고 필요하지 않은 서비스는 설치 제거한다. * 시작 응용 프로그램 목록을 검토하여 불필요한 모든 응용 프로그램이 실행되지 않도록 한다. |
| DS-6.11 | 시스템 및 시스템 구성요소의 인벤토리를 유지관리한다. | * 인벤토리는 최소한 한 달에 한 번 업데이트한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| DS-6.12 | 시스템 보안 | 네트워크 토폴로지를 문서화하고 매년 또는 인프라에 중요한 변경 사항이 있는 경우에 다이어그램을 업데이트한다. | * WAN, DMZ, LAN, WLAN(무선), VLAN, 방화벽 및 서버/네트워크 토폴로지를 포함시킨다. |
| DS-7.0 | 계정 관리 | 콘텐츠를 처리하는 모든 **정보 시스템** 및 응용 프로그램에 대해 관리자, 사용자 및 서비스 계정에 대한 계정 관리 절차를 수립 및 이행한다. | * 다음을 다루는 계정 관리 정책 및 절차를 문서화한다. * 신규 사용자 요청 * 사용자 접근 수정 * 사용자 계정의 비활성화 및 활성화 * 사용자 종료 * 계정 만료 * 휴가 * 여러 사용자가 특정 사용자 계정을 공유하는 것을 금지한다. * 서비스 계정의 사용은 필요한 응용 프로그램에만 허용한다. * 최소한 다음 인프라 시스템과 장치에 대해 로깅을 활성화한다. * 인프라 구성요소(예: **방화벽**, 인증 서버, 네트워크 운영체제, **VPN**을 포함하는 원격 접근 체제) * 제작 운영체제 * 콘텐츠 관리 구성요소(예: 저장 장치, 콘텐츠 서버, 콘텐츠 저장 도구, 콘텐츠 전송 도구) * 인터넷 접속이 가능한 시스템 * 중앙 저장소(예: syslog/로그 관리 서버, 보안 정보 및 이벤트 관리(**SIEM**) 도구)에서 로그를 관리하는 서버를 구현한다. |
| DS-7.1 | 계정 관리 | 계정 관리 활동을 추적할 수 있는 증거(예: 승인 이메일, 변경 요청 양식)를 유지 관리한다. | * 가능한 경우 모든 계정 관리 활동에 대한 운영진 승인 및 관련 조치의 증거를 유지한다. |
| DS-7.2 | 최소 권한 원칙을 사용하여 알 필요가 있는 경우에만 고유한 자격 증명서를 할당한다. | * 다음 **정보 시스템**에 대해 알 필요가 있는 경우에만 최소한으로 자격 증명서를 할당한다. * 제작 시스템 * 콘텐츠 관리 도구 * 콘텐츠 **전송 도구** * 네트워크 인프라 장치 * 로깅 및 모니터링 시스템 * 클라이언트 웹 포털 * 계정 관리 시스템(예: Active Directory, Open Directory, LDAP) * **VPN** 원격 사용 권한(절대적으로 필요한 경우에만 허용) |
| DS-7.3 | 기본 관리자 계정 및 기타 기본 계정의 이름을 변경하고 해당 자격 증명이 필요한 특정 상황(예: 운영체제 업데이트, 패치 설치, 소프트웨어 업데이트)에만 이 계정을 사용하도록 제한한다. | * 모든 하드웨어 및 소프트웨어의 사용 설명서를 참조하여 모든 기본 계정을 식별한다. * 모든 기본 계정의 비밀번호를 변경한다. * 가능한 경우, 각 계정의 사용자 이름을 변경한다. * 미사용 중인 관리자 계정은 비활성화한다. |
| DS-7.4 | 업무를 분장하여 정보 시스템에 대한 접근 권한을 할당하는 담당자가 스스로 해당 시스템의 사용자가 되지 않도록 한다(즉, 담당자는 자신에게 접근 권한을 할당할 수 없음). | * 가능한 경우 독자적 팀을 편성하여 정보 시스템에 대한 접근 권한을 부여하도록 한다. * 분장이 달성 가능하지 않은 경우 다음과 같은 보완 관리수단을 구현한다. * 회사 관계자 및 제3자 근무자의 활동을 모니터링한다. * 감사 기록지를 유지, 검토한다. * 분장을 물리적으로 구현한다. * 임원이 감독하게 한다. |
| DS-7.5 | 계정 관리 | 관리자 및 서비스 계정 활동을 모니터링하고 감사한다. | * 로깅을 지원하는 시스템 및 응용 프로그램에 대한 모니터링 관리수단을 활성화한다. * 시스템 및 응용 프로그램이 관리자 작업 및 기록을 로깅하도록 구성하고 최소한 다음 정보를 포함시킨다. * 사용자 이름 * 타임 스탬프 * 작업 * 추가 정보(작업 매개변수) * 서비스 계정을 모니터링하여 의도된 목적(예: 데이터베이스 쿼리, 응용 프로그램간 통신)으로만 사용되도록 한다. * 관리자 및 서비스 계정 활동을 매월 검토하는 절차를 구현하여 비정상 또는 수상한 동작을 식별하고 오용 가능성을 조사한다. |
| DS-7.6 | 분기마다 콘텐츠를 처리하는 모든 **정보 시스템**에 대한 사용자 접근을 검토하여 더 이상 접근이 불필요한 사용자 계정을 삭제하는 절차를 구현한다. | * **회사 관계자** 및/또는 **제3자 근무자**의 직무 역할이 변경되거나 고용이 종료되어 더 이상 접근 권한이 필요 없는 사용자의 **정보 시스템** **접근 권한**을 삭제한다. * 90일 이상 사용되지 않은 계정을 삭제하거나 비활성화한다. |
| DS-7.7 | 프로젝트 단위별로 콘텐츠에 대한 사용자 접근을 제한한다. | * 프로젝트가 완료되어 더 이상 접근이 필요 없는 사용자의 **정보 시스템** **접근 권한**을 삭제한다. |
| DS-7.8 | 계정 관리 | 기술적으로 실행이 가능한 경우 콘텐츠를 처리하는 시스템의 로컬 계정을 비활성화하거나 삭제한다. | * **정보 시스템**에 대한 사용자 접근을 인증할 수 있는 집중화된 계정 관리 서버(즉, LDAP 또는 Active Directory 등의 디렉터리 서버)를 구현한다. * 네트워크 인프라 장치의 경우, 계정 관리를 위해 AAA(인증, 권한 부여, 과금징수)를 구현한다. * 게스트 계정을 비활성화한다. * 로컬 계정을 사용해야 하는 경우, 가능하면 각 기본 계정의 사용자 이름과 비밀번호를 변경하고 로컬 계정을 사용하여 네트워크를 통해 로그인할 수 있는 기능을 비활성화한다. |
| DS-8.0 | 인증 | **정보 시스템**에 접근하는 데 **고유한 사용자 이름**과 비밀번호를 사용하도록 의무화한다. | * 모든 **정보 시스템**에 대해 **고유한 사용자 이름**과 비밀번호를 사용하도록 의무화하는 정책을 수립한다. * 최소한 **고유한 사용자 이름**과 비밀번호를 통한 인증을 요구하도록 **정보 시스템**을 구성한다. |
| DS-8.1 | **정보 시스템** 접근에 대해 강력한 비밀번호 정책을 의무화한다. | * 다음과 같이 구성된 비밀번호 정책을 마련한다. * 최소한 8자로 구성된 비밀번호 * 다음 매개변수 중 최소한 3개 포함: 대문자, 소문자, 숫자 및 특수 문자 * 최대 90일의 비밀번호 유지 기간 * 최소 1일의 비밀번호 유지 기간 * 최대 3-5회의 로그온 시도 실패 허용 * 잘못된 로그인 시도로 잠긴 사용자 계정은 수동으로 잠금이 해제되어야 하고 특정 시간이 흐른 뒤에 자동으로 잠금이 해제되지 않아야 한다. * 이전 비밀번호 10개에 대한 비밀번호 이력 |
| DS-8.2 | 인증 | 네트워크 원격 접근(예: **VPN**)에 대해 2요소 인증(예: 사용자이름/비밀번호 및 하드 토큰)을 구현한다. | * 원격 접근 시 다음 중 2개를 제공하도록 요구한다. * 개인이 알고 있는 정보(예: 사용자 이름, 비밀번호) * 개인이 가지고 있는 고유한 실제 물건(예: 토큰, **키 카드**, 스마트폰, 인증서) * 개인에게 고유한 신체/생체인식 특성(예: 지문, 망막) * 2단계 인증과 **VPN**을 128비트 이상의 고급 암호화 표준(AES)과 함께 사용하여 원격 관리 기능을 수행한다. |
| DS-8.3 | 서버 및 워크스테이션에 비밀번호로 보호되는 화면보호기 또는 화면 잠금 소프트웨어를 구현한다. | * 최대 10분 동안 활동이 없으면 비밀번호로 보호되는 화면보호기를 활성화하도록 서버 및 워크스테이션을 수동 구성하거나 정책(Active Directory 그룹 정책 등)을 통해 구성한다. |
| DS-8.4 | WAN 및 LAN/내부 네트워크 접근에 대한 계층적 인증 전략을 제공하는 추가 인증 체제의 구현을 고려한다. | * 다음 중 하나 이상을 추가하는 것을 고려한다. * 다단계 인증 * ID 및 접근 권한 관리 시스템 * 통합 인증(SSO) 시스템 * ID 통합 표준 |
| DS-9.0 | 로깅 및 모니터링 | 실시간 로깅 및 보고 시스템을 구현하여 보안 사건을 기록 및 보고한다. 최소한 다음 정보를 수집한다.   * 시간(타임 스탬프) * 위치(출처) * 당사자(사용자 이름) * 대상(콘텐츠) | * 최소한 다음 인프라 시스템과 장치에 대해 로깅을 활성화한다. * 인프라 구성요소(예: **방화벽**, 인증 서버, 네트워크 운영체제, 원격 접근 체제(예: **VPN** 시스템) * 제작 운영체제 * 콘텐츠 관리 구성요소(예: 저장 장치, 콘텐츠 서버, 콘텐츠 저장 도구, 콘텐츠 전송 도구) * 인터넷 접속이 가능한 시스템 * 응용 프로그램 |
| DS-9.1 | 중앙 저장소(예: 시스템로그/로그 관리 서버, 보안 정보 및 이벤트 관리(**SIEM**) 도구)에서 로그를 관리하는 서버를 구현한다. |  |
| DS-9.2 | 사고에 대한 적극적 대응을 촉진할 수 있도록 보안 사건이 탐지된 경우 이를 자동 통보하도록 로깅 시스템을 구성한다. | * 조사가 필요한 사건을 정의하고 해당 관계자에게 자동 통보하는 체제를 구현한다. 다음을 고려한다. * **콘텐츠/제작 네트워크** 접속의 성공적 시도 및 실패 * 콘텐츠의 비정상적 파일 크기 및/또는 전송 시간대 * 파일 무단 접근을 위한 반복 시도 * 권한 상달에서 시도 * 중앙 저장소(예: 시스템로그/로그 관리 서버, 보안 정보 및 이벤트 관리(**SIEM**) 도구)에서 로그를 집계하는 서버를 구현한다. |
| DS-9.3 | 로깅 및 보고 시스템이 보고한 비정상적 활동을 조사한다. | * 탐지된 보안 사건을 처리하는 **사고 대응** 절차를 포함시킨다. |
| DS-9.4 | 로깅 및 모니터링 | 다음에 사용되는 모든 시스템에 로깅 방법을 구현한다.   * 키 관리 * **키 관리** * 생성된 키와 추가된 인증서 모두에 대해 해당 고유 사용자를 추적할 수 있도록 한다. | * X |
| DS-9.4 | 모든 로그를 매주 검토하고 중요 및 높음은 매일 검토한다. | * 심각한 보안 사고를 의미할 수 있는 비정상적 활동을 조사한다. * 현재 통보되지 않고 있는 또 다른 비정상적 사건을 식별하여 이러한 사건에 대해 통보하도록 로깅 및 보고 시스템을 구성한다. * 서로 다른 시스템 로그의 상관 관계를 파악하여 비정상적 활동의 양상을 식별한다. * 로그 검토 결과에 기반하여 **SIEM** 설정을 적절하게 업데이트한다. |
| DS-9.5 | 콘텐츠의 내외부 이동 및 전송에 대한 로깅을 활성화하고 최소한 다음 정보를 포함시킨다.   * 사용자 이름 * 타임 스탬프 * 파일 이름 * 발신 **IP 주소** * 수신 **IP 주소** * 사건(예: 다운로드, 보기) |  |
| DS-9.6 | 로깅 및 모니터링 | 로그는 최소한 1년 동안 보존한다. | * 로그 보존에 대한 법적 규정이 있는지 결정하기 위해 법률고문의 조언을 구한다. * 특정 사용자만 접근할 수 있으며 출입 제한 구역에 위치한 중앙 서버에 콘텐츠 로그를 저장한다. |
| DS-9.7 | 로그는 해당 관계자만 접근하도록 제한한다. | * 로그 감시 및 검토를 책임지는 관계자만 로그를 볼 수 있는 권한을 갖도록 접근제한목록을 유지, 관리한다. * 업무를 분장하여 개인이 스스로의 활동을 감시하는 책임을 갖지 않게 한다. * 로그 파일에 적절한 **접근 권한**을 적용하여 로그가 무단 삭제 또는 수정되지 않도록 보호한다. |
| DS-10.0 | 모바일 보안 | 콘텐츠에 접근하거나 콘텐츠를 저장하는 모바일 장치를 위한 BYOD(Bring Your Own Device) 정책을 개발한다. | * 다음을 포함하는 모바일 장치 바이러스 백신/멀웨어 방지 보호의 구현을 고려한다. * 다음의 정의 업데이트 * 매일 검사 수행 |
| DS-10.1 | 콘텐츠에 접근하거나 콘텐츠를 저장하는 모바일 장치를 위한 승인된 응용 프로그램, 응용 프로그램 스토어 및 응용 프로그램 플러그인/확장 기능의 목록을 개발한다. | * 사전 승인된 응용 프로그램 스토어를 통해 얻지 않은 미승인 응용 프로그램 또는 승인 응용 프로그램의 설치를 금지한다. * 모바일 장치 관리 시스템을 고려한다. |
| DS-10.2 | 콘텐츠에 접근하거나 콘텐츠를 저장하는 모든 모바일 장치의 재고를 유지한다. | * 설치된 운영체제, 패치 수준, 응용 프로그램을 포함한다. |
| DS-10.3 | 전체 장치 또는 콘텐츠가 취급 또는 저장되는 장치의 구역을 암호화하도록 요구한다. | * 모바일 장치 관리 시스템을 고려한다. |
| DS-10.4 | 보안 관리수단의 우회를 방지한다. | * 탈옥, 루팅 등의 사용을 방지한다. |
| DS-10.5 | 모바일 보안 | 분실/도난/위험 노출 또는 기타 필요한 경우, 모바일 장치의 원격 삭제를 수행할 시스템을 구현한다. | * 장치를 원격으로 삭제하는 경우, 회사와 관련 없는 데이터가 손실될 수 있다는 사실을 직원들에게 상기시킨다. |
| DS-10.6 | 장치를 10분 동안 미사용 시 자동으로 잠기도록 구현한다. |  |
| DS-10.7 | 모든 모바일 장치 운영체제 패치와 응용 프로그램 업데이트를 관리한다. | * 장치 제조업체, 공급업체 또는 개발업체의 일반 공개 시 가장 최신 보안 관련 패치/업데이트를 적용한다. |
| DS-10.8 | 비밀번호 정책을 의무화한다. | * DS-8.1을 참조한다. |
| DS-10.9 | 모바일 장치의 백업 및 복원을 수행할 시스템을 구현한다. | * 백업을 암호화하고 안전한 장소에 저장한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| DS-11.0 | 보안 기술 | 보안 기법(예: 스포일링, 비시각/시각적 **워터마크 표시**)을 제공하고 지시된 경우 이를 적용하도록 한다. |  |
| DS-11.1 | 다음 중 한 방법을 통해 최소한 **AES** 128비트 이상 **암호화**를 사용하여 하드 드라이브의 콘텐츠를 암호화하거나 전체 하드 드라이브를 암호화한다.   * 파일 기반 **암호화**: (즉, 콘텐츠 자체 암호화) * 드라이브 기반 **암호화**: (즉, 하드 드라이브 암호화) | * 외장 하드 드라이브의 경우, 사전 암호화된 드라이브(예: Rocstor Rocsafe, LaCie Rugged Safe)의 구매를 고려한다. * 다음을 포함하여 하드 드라이브의 모든 콘텐츠를 암호화한다. * SAN/NAS * 서버 * 워크스테이션 * 데스크톱 * 랩톱 * 모바일 장치 * 외부 저장 드라이브 * 다음 중 하나 이상을 구현한다. * 암호화된 DMG 또는 암호화된 ZIP 파일 등의 파일 기반 **암호화** * 소프트웨어를 사용한 드라이브 기반 **암호화** |
| DS-11.2 | 대역 외 통신 프로토콜(즉, 콘텐츠 자체와 동일한 저장 **매체**에 있지 않음)을 사용하여 복호화 키 또는 비밀번호를 전송한다. | * 콘텐츠 전송에 사용된 방법과 다른 방법을 사용하여 복호화 키 또는 비밀번호를 보낸다. * 키 이름과 비밀번호는 프로젝트 또는 콘텐츠와 관련이 없도록 확인한다. |
| DS-11.3 | 보안 기술 | 다음과 같은 키 관리 정책 및 절차를 구현하고 문서화한다.   * 민감한 콘텐츠 또는 데이터를 보호할 때는 그 위치(예: 서버, 데이터베이스, 워크스테이션, 랩톱, 모바일 장치, 전송 중인 데이터, 이메일)에 상관 없이 암호화 프로토콜을 사용한다. * 콘텐츠 키의 생성, 갱신 및 회수 * 콘텐츠 키의 내외부 배포 * 필요에 따라 키 관리 절차를 개선하고 문서화한다. * 암호화 키를 식별 가능한 소유자에게 연결 * 키 관리와 키 사용을 구분하기 위한 업무 분장 * 키 보관 절차 * 키 백업 절차 | * 고객별 및 중요 자산별 고유한 암호화 키의 생산을 고려한다. * 암호 키의 무단 대체를 방지한다. * 암호 키 보유자들이 각자의 키 보유자 책임을 이해하고 수락하는 것을 공식적으로 확인하도록 한다. |
| DS-11.4 | 최소한 **AES** 128비트 이상 **암호화**를 사용하여 전체 가상 서버 인스턴스를 포함하여 움직이지 않는 콘텐츠와 움직이는 콘텐츠를 암호화한다. | * [http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1\_Dec2005.pdf](mailto:http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf) |
| DS-11.5 | 보안 기술 | 데이터/콘텐츠의 암호화에 사용된 비밀 및 개인 키(비 공개 키)는 항상 다음 형식 중 하나 이상으로 저장한다.   * 최소 데이터 암호화 키만큼 강력하고 데이터 암호화 키에서 개별적으로 저장된 키 암호화 키로 암호화 * 안전하게 암호화된 장치(예: HSM(Host Security Module) 또는 PTS(Pin Transaction Security) 상호작용 지점 장치) 내에서 * 보안 산업에서 승인된 방법에 따라 최소 두 개의 전체 길이 키 구성요소 또는 키 공유를 보유 |  |
| DS-11.6 | **신뢰할 수 있는 장치 목록(TDL)**의 장치가 올바른 소유자의 승인에 기반하여 적절한지 확인한다. | * TDL 장치에 대해서만 키 전달 메시지(KDM)를 생성한다. * X |
| DS-11.7 | 콘텐츠 키의 유효성을 확인하고 만료일이 고객의 지침을 따르는지 확인한다. | * 키가 만료되는 종료일을 지정하여 콘텐츠를 시청할 수 있는 기간을 제한한다. * 부록 A – 시설 개요 2013년 1월 1일 |
| DS-12.0 | 콘텐츠 추적 | 디지털 콘텐츠의 세부적인 추적 정보를 제공하는 디지털 콘텐츠 관리 시스템을 구현한다. | * 대여/반납된 모든 디지털 콘텐츠를 기록한다. * 모든 콘텐츠의 디지털 위치를 기록한다. * 각 예상 대여 기간을 기록한다. * 각 집행의 시간과 날짜를 기록한다. |
| DS-12.1 | 콘텐츠 추적 | 디지털 콘텐츠 이동 집행 로그는 1년 동안 보존한다. | * 다음을 포함한다. * 대여/반납 시간과 날짜 * 자산을 대여한 개인의 이름과 고유한 ID * 대여 사유 * 콘텐츠의 위치 |
| DS-12.2 | 디지털 콘텐츠 관리 시스템의 로그를 주기적으로 검토하고 이례 사항을 조사한다. |  |
| DS-12.3 | 디지털 자산 추적 시스템에 적용 가능한 경우 고객 별칭(“별칭”)을 사용한다. | * 고객 자산의 처리와 관련된 관계자에게는 고객 별칭만 알려주는 것으로 제한한다. |

| 번호 | 보안 주제 | 모범 사례 | 이행 지침 |
| --- | --- | --- | --- |
| DS-13.0 | 전송 시스템 | 움직이지 않는 콘텐츠와 움직이는 콘텐츠에 최소 **AES** 128비트 이상으로 암호화하는 접근 관리수단을 활용하고 콘텐츠 전송 세션에 강력한 인증을 사용하는 고객이 승인한 **전송** 시스템만 사용한다. | * 인가를 받은 사용자만 콘텐츠 전송 시스템에 접근할 수 있도록 허용한다. * 또한 프로젝트 기반 접근도 제한하는 것을 고려한다. * 콘텐츠 전송 시스템이 승인되었는지 사용 전에 고객과 함께 확인한다. |
| DS-13.1 | 서면으로 고객의 사전 승인을 얻어야 하는 예외 절차를 구현하여 암호화된 **전송 도구**가 사용되지 않는 상황에 대처한다. | * 인증을 위해 안전하게 전달되는 임의 생성된 사용자 이름과 비밀번호를 사용한다. * 고객이 승인한 전송 도구/응용 프로그램만 사용한다. * 암호화되지 않은 **전송 도구**를 사용해야 하는 예외 상황에 대해 고객이 승인하도록 요구한다. * 모든 예외 상황을 문서화하고 보관한다. |
| DS-14.0 | 전송 장치 방법론 | 콘텐츠 전송을 위한 전용 시스템을 구현하고 사용한다. | * 편집용 워크스테이션 및 콘텐츠 저장 서버가 콘텐츠를 직접 전송하는 데 사용되지 않도록 한다. * 전송 시스템 또는 콘텐츠를 저장, 전송 또는 조작하기 위해 사용된 시스템에 대한 **VPN**/원격 접근을 비활성화한다. |
| DS-14.1 | 콘텐츠 전송 시스템을 관리 및 제작 네트워크에서 분리한다. | * 네트워크를 물리적 또는 논리적으로 분리한다. |
| DS-14.2 | 전송 장치 방법론 | **콘텐츠/제작 네트워크**가 아닌 **비무장 지대**(**DMZ**)에 콘텐츠 전송 시스템을 둔다. | * **DMZ**에 배치하기 전에 콘텐츠 전송 시스템을 강화한다(제안 사항은 DS-1.5 참조). * 콘텐츠 **전송 도구**가 요구하는 포트를 제외한 모든 포트를 제한하는 **접근제한목록(ACL)**을 구현한다. * 내부 네트워크와 **DMZ** 간의 트래픽을 특정 발신/수신 **IP 주소**로 제한하도록 **ACL**을 구현한다. * 고객 콘텐츠를 다운로드하거나 승인된 콘텐츠 전송 위치에 접근하기 위해 필요한 접근 권한 이외에 콘텐츠를 전송하는 데 사용되는 시스템의 인터넷 접근을 비활성화한다. |
| DS-14.3 | 발신/수신에 성공한 즉시 콘텐츠 전송 장치/시스템에서 콘텐츠를 삭제한다. | * 콘텐츠 수신 시 고객이 이를 통보하도록 요구한다. * 휴지통을 포함하여 전송 장치 및 시스템에서 콘텐츠를 제거하는 절차를 구현한다. * 적용 가능한 경우, 프로젝트 완료 직후 **전송 도구**에 대한 고객의 접속을 삭제한다. * 세션 종료 후 접속이 종료되었는지 확인한다. |
| DS-14.4 | 외부로 콘텐츠 전송이 이루어지는 즉시 제작 담당 조정관에게 자동 통보한다. | * 사용자가 내부 네트워크 밖으로 콘텐츠를 보낼 때마다 제작 담당 조정관에게 자동으로 통보(예: 이메일)하도록 콘텐츠 전송 시스템을 구성한다. |
| DS-15.0 | 고객 포털 | 콘텐츠 전송, 콘텐츠 스트리밍 및 키 배포에 사용되는 웹 포털은 권한 있는 사용자만 접근하도록 제한한다. | * 다음 중 하나 이상을 실시하여 콘텐츠를 전송, 콘텐츠 스트리밍 및 키 배포에 사용되는 웹 포털에 대한 접근 제한수단을 구현한다. * 사용자 자격 증명서 요구 * 인증 및 권한 부여를 위한 장치 및/또는 사용자 키를 통합한다. * 적절한 업무 분장(예: 한 사람은 키를 생성하고 다른 사람은 이 키를 사용하여 콘텐츠를 암호화)을 통해 암호화 키를 관리한다. * 포털 접근을 특정 네트워크, **VLAN**, 서브넷 및/또는 **IP 주소** 범위로 제한한다. * 고객 포털과의 업로드/다운로드 기능을 적절하게 제한한다. |
| DS-15.1 | 고객 포털 | 고유한 자격 증명서(예: 사용자 이름 및 비밀번호)을 포털 사용자에게 할당하고 자격 증명서를 고객에게 안전하게 배포한다. | * 콘텐츠 링크에 사용자 이름과 비밀번호를 내장하지 않는다. * 사용자 자격 증명서와 콘텐츠 링크는 개별 이메일로 배포할 것을 고려한다. * 사용자 자격 증명서를 전화나 SMS로 배포하는 것을 고려한다. * 대역 외 전송을 통해 암호화 키를 배포하는 것을 고려한다. * 다음과 같이 구성된 비밀번호 정책을 마련한다. * 최소한 8자로 구성된 비밀번호 * 다음 매개변수 중 최소한 3개 포함: 대문자, 소문자, 숫자 및 특수 문자 * 최대 90일의 비밀번호 유지 기간 * 최소 1일의 비밀번호 유지 기간 * 최대 3-5회의 로그온 시도 실패 허용 * 잘못된 로그인 시도로 잠긴 사용자 계정은 수동으로 잠금이 해제되어야 하고 특정 시간이 흐른 뒤에 자동으로 잠금이 해제되지 않아야 한다. * 이전 비밀번호 10개에 대한 비밀번호 이력 |
| DS-15.2 | 사용자가 자신의 **디지털 자산**에만 접근하도록 한다(즉, 고객 A가 고객 B의 콘텐츠에 접근할 수 없게 한다). | * 최소한 분기마다 파일/디렉터리 권한을 검토하는 절차를 구현한다. * 필요한 관계자만 접근할 수 있도록 제한한다. |
| DS-15.3 | 웹 포털을 **DMZ**에 있는 전용 서버에 두고 특정 **IP** 및 프로토콜과의 통신을 제한한다. | * 고객 포털이 요구하는 포트를 제외한 모든 포트를 제한하는 **접근제한목록(ACL)**을 구현한다. * 내부 네트워크와 **DMZ** 간의 트래픽을 특정 발신/수신 **IP 주소**로 제한하도록 **ACL**을 구현한다. * **DMZ**에 배치하기 전에 시스템을 강화한다(제안 사항은 DS-1.5 참조). |
| DS-15.4 | 고객 포털 | 고객이 미리 승인한 경우가 아니면 인터넷 웹 서버에 호스팅되는 제3자의 제작 소프트웨어/시스템/서비스의 사용을 금한다. | * 다음 중 하나 이상을 추가하는 것을 고려한다. * 다단계 인증 * ID 및 접근 권한 관리 시스템 * 통합 인증(SSO) 시스템 * ID 통합 표준 * **VPN**과 128비트 이상의 고급 암호화 표준(AES)을 함께 사용한다. |
| DS-15.5 | **HTTPS**를 사용하고 내외부 웹 포털에 TLS v1가 같은 강력한 사이퍼 수트(cipher suite) 사용을 의무화한다. |  |
| DS-15.6 | 영구 쿠키 또는 자격 증명서를 보통 텍스트로 저장하는 쿠키를 사용하지 않는다. | * 기존의 웹 기반 응용 프로그램의 쿠키 사용을 검토하여 자격 증명서를 보통 텍스트로 저장하는 경우가 없도록 한다. * 응용 프로그램이 보통 텍스트로 된 쿠키에 자격 증명서를 저장하고 있는 경우 다음 중 한 조치를 취한다. * 응용 프로그램을 재구성한다. * 응용 프로그램을 업데이트한다. * 응용 프로그램 개발자에게 보안 패치를 요청한다. |
| DS-15.7 | 구성 가능한 경우, 내외부 포털 상의 콘텐츠에 대한 접근이 사전 정의된 주기마다 자동 만료하도록 설정한다. |  |
| DS-15.8 | 웹 응용 프로그램의 취약점을 분기마다 테스트하여 확인된 문제를 수정한다. | * OWASP(오픈 웹 응용 프로그램 보안 프로젝트)에서 발행한 지침 등, 업계가 인정한 검사 지침을 사용하여, XSS(교차 사이트 스크립팅), SQL 주입 공격, CSRF(교차 사이트 요청 위조) 등의 일반적 웹 응용 프로그램의 취약점을 식별한다. * 테스트는 독립된 제3자에 의해 수행되어야 한다. * 추가 정보는 부록 G를 참조한다. |
| DS-15.9 | 고객 포털 | 웹 응용 프로그램의 침투 테스트를 매년 수행하여 확인된 문제를 수정한다. | * OWASP(오픈 웹 응용 프로그램 보안 프로젝트)에서 발행한 지침 등, 업계가 인정한 검사 지침을 사용하여, XSS(교차 사이트 스크립팅), SQL 주입 공격, CSRF(교차 사이트 요청 위조) 등의 일반적 웹 응용 프로그램의 취약점을 식별한다. * 테스트는 독립된 제3자에 의해 수행되어야 한다. * 추가 정보는 부록 G를 참조한다. |
| DS-15.10 | 권한 있는 담당자만 전화통신 서비스 공급자와의 연결 설정을 요청할 수 있게 허용한다. |  |
| DS-15.11 | 이메일(웹메일 포함)을 사용한 콘텐츠의 전송을 금지한다. | * 이메일 및 첨부 파일을 암호화하는 보안 이메일 어플라이언스 서버(예: Cisco IronPort, Sophos E-Mail Security Appliance, Symantec PGP Universal Gateway Email)의 사용을 고려한다. |
| DS-15.12 | 최소한 분기마다 고객 웹 포털에 대한 접속을 검토한다. | * 프로젝트가 완료되면 고객 웹 포털로의 **접근 권한**을 삭제한다. * 비활동 계정은 삭제한다. * 데이터가 전송될 때마다 적절한 당사자에게 자동 이메일 통보를 보낼 것을 고려한다. |

부록 A — 용어집

기본 용어 및 약어에 대한 이 용어집은 본 발행물 내에서 가장 자주 사용, 언급됩니다. 이 용어 정의는 관련된 ISO 표준(27001/27002), 보안 표준(즉, NIST) 및 업계 모범 사례에서 취하였습니다. 모범 사례 지침의 본 용어집에 포함된 모든 용어는 **굵은 글씨체로 강조 표시되어 있습니다.**

| **용어 또는 약어** | **설명** |
| --- | --- |
| **접근제한목록(Access Control List: ACL)** | 자원에 접근하도록 허용된 시스템 개체의 신원을 목록화하여 시스템 자원의 접근을 제한하는 메커니즘. |
| **접근 권한** | 개체 또는 시스템을 사용/수정할 수 있는 권한. |
| **고급 암호화 표준(Advanced Encryption Standard: AES)** | NIST(미국표준기술연구소)가 개발한 대칭 키 암호화 표준으로서 128비트 블록과 128, 192, 또는 256비트의 키 길이를 사용함. |
| **자산 관리** | 취득에서부터 처분에 이르는 전체 워크플로우 내내 자산을 추적하는 시스템. |
| **폐쇄회로 텔레비전(Closed Circuit Television: CCTV)** | 제한된 수의 모니터를 통해 특정 장소로 신호를 전송하는 데 사용되는 비디오 카메라. |
| **CCTV 콘솔** | 중앙의 CCTV 감시 인터페이스 시스템. |
| **회사 관계자** | 시설에 직접 소속되어 근무하는 직원, 임시 근무자, 인턴 등의 개인. |
| **콘텐츠/ 제작 네트워크** | 매체 콘텐츠의 저장, 전송, 또는 처리에 사용되는 컴퓨터 네트워크. |
| **디지털 자산** | 사용 권한을 포함하는 2진 소스 형식으로 된 일체의 콘텐츠 및/또는 매체. |
| **실사** | 채용 전에 잠재적 직원 또는 제3자 근무자의 평판이 좋은지 확인하는 연구 또는 조사. |
| **동적 호스트 설정 통신규약(Dynamic Host Configuration Protocol: DHCP)** | 네트워크 상의 모든 노드에 IP 주소를 자동 할당하는 데 사용되는 통신규약. |
| **비무장 지대(Demilitarized Zone: DMZ)** | 조직의 외부 서비스를 포함하면서 이를 더 큰 규모의 신뢰할 수 없는 네트워크(보통 인터넷)로 노출시키는 물리적 또는 논리적 서브 네트워크. |
| **암호화** | 권한 없는 사람이 쉽게 이해할 수 없는 암호문 형태로의 데이터 변환. |
| **핑거프린팅** | 소프트웨어가 매체의 특징적 구성요소를 식별, 추출 및 압축하는 기술로서, 압축된 결과적 형태에 의해 해당 매체의 고유한 식별이 가능해진다. |
| **방화벽** | 로컬 보안 정책에 따라 네트워크 간 접속을 제한하는 게이트웨이. |
| **방화벽 규칙** | 소스와 대상 간의 패킷 라우팅 방법을 판단하기 위해 방화벽이 사용하는 지시표. |
| **FireWire** | 외부 장치로부터 컴퓨터로 데이터를 전송할 수 있게 하는 고속 인터페이스. |
| **파일 전송 프로토콜(File Transfer Protocol: FTP)** | 비암호화 상태로 네트워크 상의 파일 전송을 지정하는 TCP/IP 프로토콜. |
| **HTTPS** | 컴퓨터 네트워크에서 보안 통신을 위한 통신 프로토콜로 특히 인터넷에 광범위하게 배포됨. |
| **신분 확인증** | 시설을 출입하도록 허가된 사람(예: 직원, 업체, 방문객)을 식별하는 데 사용하는 카드. |
| **침입 탐지/침입 차단(IDS/IPS)** | 침입 탐지 시스템(IDS)은 장치 또는 소프트웨어 응용 프로그램으로 네트워크 또는 시스템 활동에서 악의적인 활동이나 정책 위반을 모니터링하고 관리 스테이션에 보고서를 작성하여 제출한다. 침입 차단 시스템(IPS)도 같은 기능을 수행하고 활동 차단까지 시도한다. |
| **사고 대응** | 보안 사고의 탐지, 분석 및 시정. |
| **정보 시스템** | 시설 측에서 정보를 처리하는 데 사용하는 전자식 또는 컴퓨터 기반 시스템. 정보 시스템에는 응용 프로그램, 네트워크 장치, 서버, 워크스테이션 등이 포함된다. |
| **입출력 장치** | 컴퓨터와의 통신 및/또는 컴퓨터 간 통신에 사용되는 장치(예: USB 및 FireWire 드라이브). |
| **IP 주소** | 컴퓨터 네트워크에 참여하는 장치에 할당된 숫자 형식의 식별자(논리 주소). |
| **키 관리** | 암호화된 콘텐츠에 접근하는 데 사용되는 암호 키의 생성, 배포, 저장 및 회수. |
| **키 카드** | 전자식으로 출입을 제어하는 잠금 장치에 사용되며, 디지털 서명을 저장하고 있는 플라스틱 카드. |
| **근거리 통신망(Local Area Network: LAN)** | 소규모의 물리적 공간(예: 사무실)을 동작 범위로 한 컴퓨터 네트워크. |
| **MAC 주소 필터링** | 컴퓨터 네트워크로의 접속을 제한하는 데 사용되는 보안 접근 제어 방법론. |
| **마스터 열쇠** | 특정 시설의 모든 출입문(내외부)에 대해 접근을 제공하는 키. 보안 수준이 높은 모든 구역을 출입할 수 있는 열쇠이며, 마스터 열쇠로도 간주된다. |
| **매체** | 자기 테이프, 광 디스크, 자기 디스크, LSI 메모리칩, 정보가 기록, 저장, 또는 출력된 인쇄물을 포함하여 이에 국한되지 않는 정보 시스템 내의 물리적 장치나 필기 지면. |
| **네트워크 프로토콜** | 전산의 종점 간 연결, 통신 및 데이터 전송을 제어하거나 활성화하는 규약 또는 표준. |
| **네트워크 인터페이스 카드(NIC)** | 컴퓨터를 컴퓨터 네트워크에 연결하는 컴퓨터 하드웨어 구성요소. |
| **비제작 네트워크** | 매체 콘텐츠를 처리하거나 전송하는 데 사용되지 않는 모든 컴퓨터 네트워크. 비제작 네트워크에는 사내망 또는 관리망과 고객 네트워크가 포함될 수 있다. |
| **위험 평가** | 회사에 미칠 수 있는 잠재적 위험을 식별하기 위한 위험의 식별 및 우선순위화. |
| **위험 관리** | 위험 평가를 통한 위험의 식별, 분석, 완화 및 보안 관리수단의 구현. |
| **라우터** | 해당 소프트웨어 및 하드웨어가 정보의 방향 지정과 전달 작업에 맞춰진 장치. |
| **보안 정보 및 이벤트 관리(SIEM)** | 보안 정보 관리(SIM)와 보안 이벤트 관리(SEM)를 결합한 소프트웨어 제품 및 서비스에 대한 용어. SIEM 기술은 네트워크 하드웨어와 응용 프로그램에 의해 생성된 보안 경고에 대한 실시간 분석 기능을 제공한다 |
| **업무 분장** | 한 사람이 특정 작업을 혼자 완료할 수 있는 능력을 갖지 않도록 하는 보안 원칙. 한 사람이 하나 이상의 관련 직무에 대해 책임질 수 없도록 하는 원칙. |
| **서비스 집합 ID(SSID)** | 종종 사람이 읽을 수 있는 문자열이기도 해서 보통 "네트워크 이름"으로 불리는 무선 LAN의 고유한 식별자. |
| **소형 컴퓨터 시스템 인터페이스(Small Computer System Interface: SCSI)** | 컴퓨터와 주변장치 간의 물리적 연결 및 데이터 송수신을 위한 표준. |
| **중간대기 구역** | 배달이나 입수 등을 위해 집배되기 전에 콘텐츠를 저장하는 공간. |
| **정적 IP 주소** | 컴퓨터가 작동될 때마다 동일한 IP 주소를 사용하는 구성. |
| **스위치** | 네트워크 내 복수의 장치를 연결하여 특정 목적지로 트래픽을 전송하는 컴퓨터 네트워킹 장치. |
| **텔넷** | 원격 장치에 접속하기 위해 인터넷 또는 근거리 통신망(LAN)에서 사용하는 네트워크 프로토콜. |
| **제3자 근무자** | 외부 회사에 소속되어 있으나 용역을 제공하도록 시설 측이 채용한 일체의 개인. 제3자 근무자에는 계약직원, 프리랜서, 파견업체 등이 포함된다. |
| **추적 체제** | 자산 등록, 자산 이동 추적(예: 금고실에서 편집 구역으로 자산의 이동), 운송 및 자산 파기를 포함한 전 제작 과정 내내 자산을 추적하는 데 사용되는 도구, 절차 및/또는 수단. |
| **전송 도구** | 보통 허용 가능한 암호화 및 인증 체제를 통해 네트워크 상에서 디지털 자산을 전자적으로 전송하는 데 사용되는 도구. |
| **전송 프로토콜** | 컴퓨터 네트워크 또는 인터넷 상에서 파일을 전송하는 것과 관련된 절차. |
| **신뢰할 수 있는 장치 목록(Trusted Device List: TDL)** | 콘텐츠를 재생하도록 승인된 특정 디지털 장치 목록. |
| **고유한 사용자 이름** | 구별 가능한 로그인 식별자. |
| **유니버설 시리얼 버스(Universal Serial Bus: USB)** | 장치를 호스트 컴퓨터와 연결하기 위한 직렬 버스 표준. |
| **사용자 접근 관리** | 접근 권한을 생성, 변경하고, 시스템이나 응용 프로그램에서 사용자 계정을 삭제하는 절차. |
| **금고실** | 콘텐츠가 포함된 물리적 매체를 보관하기 위한 전용 공간. |
| **가상 근거리 통신망(Virtual Local Area Network: VLAN)** | LAN/내부 네트워크의 특성을 가지고 있으나 물리적 위치에 국한되지 않는 컴퓨터 네트워크. |
| **가상 사설 통신망(Virtual Private Network: VPN)** | 사용자가 보다 큰 규모의 다른 네트워크에 접속하도록 허용하는 컴퓨터 네트워크. |
| **광역 통신망(Wide Area Network: WAN)** | 광역(예: 회사)을 동작 범위로 포함하는 컴퓨터 네트워크. |
| **워터마크 표시** | 디지털 자산에 (거의) 불가역적인 정보를 내장하는 절차. |
| **작업 진행 중(Work in Progress: WIP)** | 최종 상품으로 간주되는 않는 상품. |
| **워크플로우** | 회사가 콘텐츠에 대해 수행하는 일련의 작업 단계. |

부록 B — MPAA 제작물 및 배포 경로 정의

**제작물 종류**

| **제작물 종류** | **설명** |
| --- | --- |
| **피처** | 극장 개봉되거나 홈 비디오 또는 인터넷으로 바로 출시되는 제작물로 다음 유형을 포함한다.   |  |  | | --- | --- | | **피처 종류** | **설명** | | 피처 필름 | 장편 영화. | | 단편 | 피처 필름으로 간주되는 것보다 길이가 짧은 영화. | | 피처외 장편 | 다큐멘터리 등의 기타 제작물. | |
| **TV 에피소드** | TV, 웹, 또는 모바일과 관련된 제작물로서 시즌 또는 미니시리즈의 에피소드를 포함한다. 파일럿을 비롯하여 기타 특별 시리즈(“웨비소드” 또는 “모비소드” 등)도 에피소드에 해당한다. |
| **TV 에피소드 외** | TV, 웹, 또는 모바일과 관련된 제작물로서 에피소드를 포함하지 않는 제작물(예: 텔레비전용 영화, 스포츠 행사, 또는 뉴스 프로그램). |
| **홍보/광고** | 다음을 포함하는 제작물:   * + “홍보” – 미디어와 관련된 모든 홍보물. 여기에는 티저, 트레일러, 전자식 보도 자료 및 기타 자료가 포함된다. 홍보는 ‘광고’의 특별한 경우이다. |
| **광고** | TV 광고, 정보광고, 공익광고 및 “홍보”에 포함되지 않는 홍보를 포함하는 광고 형태. 여기에는 TV 광고로 방송될 수도 있는 영화 트레일러와 티저가 포함되지 않는다. |
| **음악** | 통화연결음, 뮤직비디오 및 기타 음악을 포함하는 제작물. |
| **기타** | 다음을 포함하는 제작물:   |  |  | | --- | --- | | **종류** | **설명** | | 발췌 | 다른 작품의 일부가 대부분을 구성하는 자산. | | 부록 | 다른 작품의 보충으로 제작된 자료. DVD와 연관된 증간물을 예로 들 수 있다. | | 컬렉션 | 다른 범주에 들어가지 않는 자산의 집합. 영화 컬렉션을 예로 들 수 있다. | | 프랜차이즈 | 다른 종류의 작품 컬렉션이나 이의 조합으로서, 예를 들어 프랜차이즈에는 복수의 TV 쇼, 또는 TV 쇼와 영화가 포함될 수 있다. | |

**배포 경로**

| **배포 경로** | **설명** |
| --- | --- |
| **극장** | 피처 필름은 독점적으로 극장에만 개봉된다. |
| **극장 외** | 영화가 텔레비전, 홈 비디오 또는 극장 이외의 방식으로 일반에 공개된다. 예를 들어 영화가 (i) 비행기, 기차, 배 및 기타 일반 교통수단, (ii) 학교, 대학교 및 기타 교육기관, 도서관, 정부기관, 기업, 서비스 조직 및 클럽, 교회 및 기타 종교 단체, 박물관 및 영화단체에서 상영되고(상영지의 주변 지역 내에서 폐쇄 회로에 의한 상영의 전송을 포함함), (iii) 상설 또는 임시의 군사시설, 격리 시설, 교도소, 은퇴 센터, 역외의 반잠수형 굴착선, 벌목장, 원거리의 산림 및 건설 현장에서 상영될 수 있다(상영지의 주변 지역 내에서 폐쇄 회로에 의한 상영의 전송을 포함함). |
| **홈 비디오** | 영화가 DVD나 Blu-Ray 등의 형태로 포장 상품의 도매급 실판매 및 대여 판매를 위해 출시된다. |
| **무료 텔레비전** | 영화가 대개 네트워크, 텔레비전 방송국, 또는 기본 케이블 네트워크와의 사용권 계약에 명시된 대로 무료 공중파를 통해 일반에 공개된다. |
| **유료 텔레비전** | 방송망 내 최소한 한 참여자가 사용료를 지급할 것을 조건으로 영화가 일반에 공개되며, 주문형 비디오, 케이블, 위성 및 유료 시청제를 예로 들 수 있다. |
| **인터넷** | 영화가 다음의 온라인 배포 경로 중 하나로 개봉된다.   |  |  | | --- | --- | | **종류** | **설명** | | 온라인 다운로드 판매(Electronic Sell-Through: EST) 또는 영화 내려받기 서비스(Download to Own: DTO) | 영구적인 디지털 사본이 온라인으로 판매됨. | | 온라인 대여 또는 주문형 비디오(Video-on-Demand: VOD) | 임시 시청을 위한 온라인 유료 대여. | | 정액제 주문형 비디오(Subscription Video-on-Demand: SVOD) | 온라인 가입형 대여를 통한 온라인 시청. | | 온라인 무료 주문형 비디오(Free Video-on-Demand: FVOD) | 보통 광고 수익으로 지원되는 무료 온라인 스트리밍 시청. | | 기타 | 모바일이나 IPTV(인터넷 프로토콜 TV) 등의 온라인 및 뉴 미디어. | |

부록 C - 시설에 대한 매핑

각 시설은 용례를 검토하여 시설이 제공하는 서비스에 해당하는 시설 종류를 식별한 다음, 위험 평가 결과를 바탕으로 적절한 관리수단을 이행해야 합니다.

|  |  |  |  |
| --- | --- | --- | --- |
| **ADS** | | | |
| ADS | 음성 시설은 제작 과정 중에 녹음되는 음향의 처리와 추가적인 음향 효과 및 악보 제작을 통한 음향의 증강을 담당한다. | FL | CDF |
| CA | 크리에이티브 광고 | IFE | D |
| CDF | IFE | PP | DC |
| D | 배포 | R | 복사 |
| DC | R | 번호 | 번호 |
| DS | VFX | AS | 응용 프로그램 보안 |
| DVD | CA | CS | 클라우드 보안 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| MS-1.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| MS-5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-6.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-6.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-7.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-8.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-8.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-9.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-10.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-11.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-11.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.6 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-1.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-1.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-1.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-4.1 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-4.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-4.3 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.6 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.7 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-6.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-6.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-6.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-10.0 | X | X | X | X | X | X | X | X | X | X |  | X | X | X |
| PS-10.1 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-10.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-10.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-11.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-11.1 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.3 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.4 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.5 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.6 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.7 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.8 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-11.9 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-12.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-12.1 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.2 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.3 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.4 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.5 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.6 |  |  | X | X |  |  |  |  |  |  |  |  |  |  |
| PS-13.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-13.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-14.0 | X | X |  | X | X | X | X | X | X | X | X | X |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-14.1 | X | X | CDF | X | X | X | X | X | X | X | X | X | AS | CS |
| PS-14.2 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-15.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.3 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| PS-15.4 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| PS-16.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.5 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-17.6 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-17.7 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-17.8 |  |  |  |  |  |  |  | X |  |  | X |  |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-17.9 |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| PS-18.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-18.1 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-18.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-18.3 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-19.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-20.0 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-20.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-20.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-21.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-21.1 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-21.2 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-21.3 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| DS-1.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-1.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-4.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-4.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-4.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-5.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-5.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-7.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-10.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.6 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| DS-11.7 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| DS-12.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-13.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-13.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-14.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |

부록 D - 관리수단의 매핑 참고자료

보안 관리수단을 구현할 때 추가 정보가 필요한 경우 이 표준을 참고할 수 있습니다. 제시된 보안 관리수단을 구현할 때 추가 정보가 필요한 경우 이 표준을 참고할 수 있습니다.

| **보안 주제** | **ISO 27002 참조** | **ISO 27002 -2013 참조** | **NIST 800-53 Rev. 4 참조** |
| --- | --- | --- | --- |
| **MS-1.0** | 운영진의 보안 인식/감독 | 6.1.1 | MS.S-3.0 |
| **MS-1.1** | 6.1.1 | AT-2, AT-3, PM-1, PM-2 |
| **MS-1.2** | 5.1.2, 6.1.1 | PM-1, PM-6, AT-3 |
| **MS-1.3** | 5.1.2, 6.1.1 | PM-1, PM-6, AT-3 |
| **MS-2.0** | 위험 관리 | 6.1.1 | CA-1, RA-1 |
| **MS-2.1** | 5.1.2 | RA-2 |
| **MS-3.0** | 보안 조직 | PE-6, PM-2, SI-4 | PM-2 |
| **MS-4.0** | 정책 및 절차 | 5.1.1, 6.1.1 | PL-1 |
| **MS-4.1** | 5.1.2 | PL-1 |
| **MS-4.2** | 8.1.3 | PL-1, PS-7 |
| **MS-4.3** | 8.2.2, 8.1.3 | AT-1, AT-2, AT-3, AT-4 |
| **MS-5.0** | 사고 대응 | 16.1.1 | IR-1, IR-8 |
| **MS-5.1** |  | IR-2 |
| **MS-5.2** | 16.1.2 | IR-6, IR-7 |
| **MS-5.3** | 16.1.2 | IR-4, IR-5 |
| **MS-6.0** | 사업 연속성 및 재해 복구 | 17.1.1 | CP |
| **MS-6.1** | 17.1.1 | CP |
| **MS-7.0** | 변경 제어 및 구성 관리 | 14.2.2 | CM |
| **MS-8.0** | 워크플로우 | 11.1 |  |
| **MS-8.1** | 11.1 |  |
| **MS-9.0** | 업무 분장 | 6.1.2 | AC-5 |
| **MS-10.0** | 신원 조회 | 7.1.1 | PS-3 |
| **MS-11.0** | 기밀유지 계약 | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-11.1** | 8.1.4 | PS-4, PS-8 |
| **MS-12.0** | 제3자의 이용 및 적격심사 | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-12.1** | 8.1.4 | PS-7, SA-9 |
| **MS-12.2** | 7.2.1 | PS-4 |
| **MS-12.3** | 8.14 |  |
| **MS-12.4** | 7.1.2 | PS-7 |
| **MS-12.5** | 11.1.2 | PL-4, PS-6, SA-9 |
| **MS-12.6** | 7.1.1 |  |
| **PS-1.0** | 출입 지점 | 11.1 | PE-3 |
| **PS-1.1** | 11.1 | PE-3, PE-6 |
| **PS-1.2** | 11.1 | PE-1, PE-2, PE-3 |
| **PS-2.0** | 방문객 출입 | 11.1 | PE-8 |
| **PS-2.1** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-2.2** | 11.1 | PS.S-6.0 |
| **PS-2.3** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-3.0** | 신분 확인 | 11.1.2 | PE-3 |
| **PS-4.0** | 경계 보안 | 11.1.1 | PE-3 |
| **PS-4.1** | 11.1.1 | PE-3 |
| **PS-4.2** | 11.1.1 | PE-3 |
| **PS-4.3** | 11.1.1 | PE-3 |
| **PS-5.0** | 경보 | 11.1.1 | PE-3, PE-6 |
| **PS-5.1** |  | PE-6 |
| **PS-5.2** | 11.1.1 | AC-6 |
| **PS-5.3** | 11.1.1 |  |
| **PS-5.4** | 11.1.1 | PE-3, PE-6 |
| **PS-5.5** | 11.1.1 | PE-3 |
| **PS-5.6** | 11.1.1 | PE-6 |
| **PS-5.7** | 11.1.1 | PE-9, PE-10, PE-11, PE-13 |
| **PS-6.0** | 권한 부여 | 11.1 | PE-1, PE-2, PE-3 |
| **PS-6.1** | 11.1 | PE-2, |
| **PS-6.2** | 11.1 | PE-2, PS-4, PS-5 |
| **PS-7.0** | 전자식 출입 제어 | 11.1 | PE-2, PE-3 |
| **PS-7.1** | 11.1 | PE-2, PE-3 |
| **PS-7.2** | 11.1 | PE-2, PE-3 |
| **PS-7.3** | 11.1 | PE-2, PE-3 |
| **PS-7.4** | 11.1 | PE-2, PE-3 |
| **PS-8.0** | 열쇠 | 11.1 | PE-2, PE-3 |
| **PS-8.1** | 11.1 | PE-2, PE-3 |
| **PS-8.2** | 11.1 | PE-2, PE-3 |
| **PS-8.3** | 11.1 | CM-8 |
| **PS-8.4** | 9.2.6 | CM-5, CM-8 |
| **PS-8.5** | 9.2.6 | CM-5, CM-8 |
| **PS-9.0** | 카메라 |  | PE-6 |
| **PS-9.1** | 11.1 | PE-6 |
| **PS-9.2** | 11.1 | PE-2, PE-3 |
| **PS-9.3** | 11.1 | AU-6, PE-6 |
| **PS-9.4** | 11.1 | PE-6 |
| **PS-10.0** | 로깅 및 모니터링 | 12.4 | AU-3, AU-6  AU-9, AU-11 |
| **PS-10.1** | 12.4 | AU-6 |
| **PS-10.2** | 12.4 | AU-6 |
| **PS-11.0** | MP-3 | 11.1 |  |
| **PS-11.1** |  |  |
| **PS-11.2** |  |  |
| **PS-11.3** |  |  |
| **PS-11.4** |  |  |
| **PS-11.5** |  |  |
| **PS-11.6** | 11.1 |  |
| **PS-11.7** |  |  |
| **PS-11.8** |  |  |
| **PS-11.9** |  |  |
| **PS-12.0** | SI-5 | 8.1 | CM-8 |
| **PS-12.1** | 8.2.2 | MP-3 |
| **PS-12.2** | 8.2.3 | AU-9, AU-11 |
| **PS-12.3** |  | AU-6, CM-8 |
| **PS-12.4** |  |  |
| **PS-12.5** | 8.2.3 | AU-1, AU-3, AU-6 |
| **PS-12.6** | 8.2.3 |  |
| **PS-13.0** | 재고 합계 | 8.1.1 | AU-6, CM-8 |
| **PS-13.1** | 6.1.2 | AC-5 |
| **PS-14.0** | PS.S-15.0 | 8.2.2 | MP-4 |
| **PS-14.1** | 8.1.1 | MP-4, PE-2, PE-3 |
| **PS-14.2** |  |  |
| **PS-15.0** | 고객 자산 | 8.2.3 | MP-4, PE-2, PE-3 |
| **PS-15.1** | 8.2.3 | MP-2, MP-4 |
| **PS-15.2** |  |  |  |
| **PS-15.3** |  |  |  |
| **PS-15.4** |  |  |  |
| **PS-16.0** | 처분 | 8.3.2 | MP-6 |
| **PS-16.1** | 8.3.2 | MP-6 |
| **PS-16.2** |  | MP-6 |
| **PS-16.3** |  | MP-6 |
| **PS-16.4** |  |  |
| **PS-17.0** | 운송 | 8.3.3 | MP-5 |
| **PS-17.1** | 8.3.3 | AU-11, PE-16, MP-5 |
| **PS-17.2** | 8.2.3 | MP-5 |
| **PS-17.3** | 8.3.3 | PE-3, PE-7 |
| **PS-17.4** | 8.3.3 | PE-3, PE-7 |
| **PS-17.5** |  |  |
| **PS-17.6** |  |  |
| **PS-17.7** |  |  |
| **PS-17.8** |  |  |
| **PS-17.9** |  |  |
| **PS-18.0** | 수취 | 8.2.3 | PE-16 |
| **PS-18.1** |  | MP-5 |
| **PS-18.2** | 8.2.2 | MP-3, MP-4 |
| **PS-18.3** | 8.2.3 | MP-3, MP-5 |
| **PS-19.0** | 라벨 부착 | 8.2.2 | MP-3 |
| **PS-20.0** | 포장 | 8.3.3 | MP-5 |
| **PS-20.1** | 8.3.3 |  |
| **PS-20.2** |  |  |
| **PS-21.0** | PS.S-21.1 |  | MP-5 |
| **PS-21.1** |  |  |
| **PS-21.2** |  |  |
| **PS-21.3** |  |  |
| **DS-1.0** | 외부 네트워크/WAN | 13.1 | AC-4, SC-7 |
| **DS-1.1** | 9.1, 13.1, 13.2 | AC-3, AC-4 |
| **DS-1.2** | 10.1, 13.2 | CM-7 |
| **DS-1.3** | 13.2 | AC-20, CA-3, SC-7 |
| **DS-1.4** | 12.6 | CM-6, SI-2 |
| **DS-1.5** |  | CM-6, CM-7 |
| **DS-1.6** | 9.4, 10.1 | AC-6, AC-17 |
| **DS-1.7** | 12.3, 17.1 |  |
| **DS-1.8** | 12.6, 13.1 | RA-5, SC-7 |
| **DS-1.9** | 12.6 | RA-5, SC-7 |
| **DS-1.10** | 10.1, 13.1 | SC-7, SC-12, SC-33 |
| **DS-1.11** | 12.4 | SC-7, SC-12, SC-33 |
| **DS-1.12** | 12.2, 16.1 | SC-7, SC-12, SC-33 |
| **DS-2.0** | 인터넷 | 12.1, 13.1 | CA-3 |
| **DS-2.1** | 13.2 | PL-4 |
| **DS-2.2** | 13 | AC-6, PL-4 |
| **DS-3.0** | LAN/내부 네트워크 | 9.4, 13.1 | SC-7 |
| **DS-3.1** | 11.2 |  |
| **DS-3.2** | 6.2, 13.1, 9 | AC-3, AC-17 |
| **DS-3.3** | 10.1 | CM-6, CM-7 |
| **DS-3.4** | 13.1 | SC |
| **DS-3.5** | 13.1 | SC |
| **DS-3.6** | 16.1 | SI-4 |
| **DS-3.7** | 9.4 | SC |
| **DS-3.8** | 9.1 | SC |
| **DS-3.9** | 12.6 | SC |
| **DS-3.10** | 12.3, 17.1 | SC |
| **DS-4.0** | 무선 | 9.1, 13.1 | AC-18 |
| **DS-4.1** | 9.1, 13.1 | AC-18 |
| **DS-4.2** | 9.1, 13.1 | SI-4 |
| **DS-5.0** | 입출력 장치 보안 | 10.7.1 | SC-7 |
| **DS-5.1** |  | AC-19, MP-2 |
| **DS-6.0** | 시스템 보안 | 12.2 | SI-3 |
| **DS-6.1** | 12.2 | SI-3 |
| **DS-6.2** | 12.2 | SI-3 |
| **DS-6.3** | 12.2 | SI-3 |
| **DS-6.4** | 12.5, 12.6 | SI-2, RA-5 |
| **DS-6.5** | 9.4 | AC-5, SC-2 |
| **DS-6.6** | 11.2 | PE-3 |
| **DS-6.7** | 6.2, 10.1, 11.1 | MA-4, PE-5 |
| **DS-6.8** | 8.1, 12.5 | CM-11 SI-7 |
| **DS-6.9** | 12.1, 12.5 | CM-10, SI-7 |
| **DS-6.10** | 12.6 | AC-3, AC-6, CM-7 |
| **DS-6.11** | 8.1 | CM-8 |
| **DS-6.12** | 8.1, 14.1, 14.2 |  |
| **DS-7.0** | 계정 관리 | 9 | AC-2 |
| **DS-7.1** | 9.1 | AC-2 |
| **DS-7.2** | 9.2, 9.4 | AC-2, AC-6, IA-4 |
| **DS-7.3** | 8.1, 9.2, 9.4 | AC-2, AC-6, IA-4 |
| **DS-7.4** | 12.4, 18.2 | AC-2, AC-6, IA-4 |
| **DS-7.5** | 12.1, 12.4 | AU-3, AU-6 |
| **DS-7.6** | 9.2, 9.4 | AU-2, AU-12 |
| **DS-7.7** | 9.2, 9.4 | PS-4, PS-5 |
| **DS-7.8** | 9.2, 9.4 | AC-2, PE-2 |
| **DS-8.0** | 인증 | 9.1 | IA-2, IA-4 |
| **DS-8.1** | 9 | AC-7, IA-5 |
| **DS-8.2** | 9.4, 10.1 | AC-17 |
| **DS-8.3** | 9.2, 9.4 | AC-11 |
| **DS-8.4** | 9.4 | AC-1 |
| **DS-9.0** | 로깅 및 모니터링 | 12.4 | SI-4, AU-2, AU-3 |
| **DS-9.1** | 12.4 | AU-1, AU-6 |
| **DS-9.2** | 12.4 | AU-1, AU-6 |
| **DS-9.3** | 12.4 | AU-1, AU-2, AU-6 |
| **DS-9.4** | 10.1 | AU-2, AU-3 |
| **DS-9.5** | 12.4 | AU-3, AU-8 |
| **DS-9.6** | 10.1.3, 10.10.3 | AU-9, AU-11 |
| **DS-9.7** | 12.4 | AU-6 |
| **DS-10.0** | 모바일 보안 | 6.2, 11.2 | SC, AC, IA-2 |
| **DS-10.1** | 6.2, 11.2 | SC, AC |
| **DS-10.2** | 6.2, 11.2 | SC, AC |
| **DS-10.3** | 6.2, 11.2 | SC, AC |
| **DS-10.4** | 6.2, 11.2 | SC, AC |
| **DS-10.5** | 6.2, 11.2 | SC, AC |
| **DS-10.6** | 6.2, 11.2 | SC, AC |
| **DS-10.7** | 6.2, 11.2 | SC, AC |
| **DS-10.8** | 6.2, 11.2 | SC, AC |
| **DS-10.9** | 6.2, 11.2 | SC, AC |
| **DS-11.0** | 보안 기술 | 8.2, 10.1 |  |
| **DS-11.1** | 8.2, 10.1 | IA-5, SC-13 |
| **DS-11.2** | 8.2, 10.1 | SC-8, SC-12 |
| **DS-11.3** | 8.2, 10.1 | SC-12 |
| **DS-11.4** |  |  |
| **DS-11.5** |  |  |
| **DS-11.6** | 10.1 |  |
| **DS-11.7** | 10.1 |  |
| **DS-12.0** | 콘텐츠 추적 |  |  |
| **DS-12.1** |  |  |  |
| **DS-12.2** |  |  |  |
| **DS-12.3** |  |  |  |
| **DS-13.0** | 전송 시스템 | 10.1, 13.2 | IA-5, SC-13 |
| **DS-13.1** | 10.1, 13.2 |  |
| **DS-14.0** | 전송 장치 방법론 | 13.1 |  |
| **DS-14.1** | 13.1 | AC-4, SC-7 |
| **DS-14.2** | 13.1 | AC-4, AC-20, SC-7 |
| **DS-14.3** | 13.2 | MP-6 |
| **DS-14.4** | 12.4, 13.2 |  |
| **DS-15.0** | 고객 포털 | 13.1 | AC-6 |
| **DS-15.1** | 9.2, 9.4 | IA-5 |
| **DS-15.2** | 9.2, 9.4 | AC-2, AC-3, AC-6 |
| **DS-15.3** | 12.6, 13.1 | AC-4, AC-20 |
| **DS-15.4** | 9.2, 9.4, 10.1 |  |
| **DS-15.5** | 10.1 | SC-8, SC-13 |
| **DS-15.6** | 9.4 | AC-4 |
| **DS-15.7** | 9.4 | AC-2 |
| **DS-15.8** | 12.6 | SI-7 |
| **DS-15.9** | 12.6 |  |
| **DS-15.10** |  |  |
| **DS-15.11** | 13.2 | AC-4 |
| **DS-15.12** | 12.1 |  |

부록 E - 자주 묻는 질문

1. **저희 시설에서 제안된 모범 사례를 모두 이행해야 합니까?**

모범 사례의 준수는 전적으로 자유 의사에 따릅니다. 모범 사례는 보안 절차를 수립, 이행, 수정할 때 고려할 수 있도록 제안된 지침입니다.

1. **저희 시설에서 복수의 서비스(예: 필름 현상 및 포스트 프로덕션)를 제공할 경우, 어떤 모범 사례 보완 지침을 적용해야 합니까?**

작업 절차가 서로 분장되어 있지 않는 한 시설에서는 좀 더 제한적인 모범 사례 보완 지침을 항상 적용해야 하며, 이 경우 해당 서비스를 위한 환경에 모범 사례 보완 지침만을 적용해야 합니다.

1. **저희 시설에서 모범 사례의 “이행 지침” 섹션에 포함된 모든 사항을 적용해야 합니까?**

아니요. 이행 지침 섹션에 포함된 정보는 특정 보안 관리수단을 체계화하는 최선의 방법을 결정하는 데 도움을 주기 위해 작성되었습니다. 해당 시설이 MPAA가 실시하는 콘텐츠 보안 평가에 응할 경우, 당사의 평가는 오직 특정 시점의 시설 관행을 지침 내 해당 모범 사례와 비교하기만 합니다. (MPAA 콘텐츠 보안 평가를 받는 제세한 방법은 contentsecurity@mpaa.org로 문의하십시오.

1. **저희 현재 시스템에서 모범 사례의 구현이 불가능한 경우는 어떻게 합니까?**

시스템이 모범 사례를 구현하는 데 필요한 가능한 솔루션을 알아보려면 해당 시스템 업체에게 문의하시기 바랍니다. 해결 방안에는 패치 적용, 버전 업데이트 또는 보안이 강화된 시스템으로의 변경 등이 있을 수 있습니다. 기술적 한계로 인해 모범 사례를 구현할 수 없는 경우 대안적 보안 수단을 사용할 수도 있으나, 이는 일반적으로 관련 위험에 대한 대처로 간주되지 않습니다. 시스템 한계에 따른 보안 지침 이행의 예외 사항은 공식적으로 문서화하여 고객의 승인을 받아야 합니다.

1. **이 지침의 모범 사례를 적용할 때, 저희 시설에서 MPAA 회원사가 별도로 명시한 보안 요구사항을 준수해야 합니까?**

모범 사례의 이행은 지침으로서, 시설이 개별 MPAA 회원사와 맺은 계약에 따른 특정 조항을 대체하지 않습니다. 특정 회원사의 업체 이용에 관한 결정은 각 회원사가 일방적으로 정합니다. MPAA는 보안에 대한 고객과의 향후 논의 시 본 모범 사례를 지침으로 활용하도록 권장합니다.

부록 F - 권장 정책 및 절차

다음은 콘텐츠 보호를 위해 보안 정책 및 절차의 수립과 이행이 필요한 일반적인 분야의 예입니다.

1. **물리적 보안 정책 및 절차**

* 출입 지점 보안
* 방문객 출입 프로토콜
* 신원확인 및 권한 부여
* 긴급상황 프로토콜
* 시설 출입 관리수단
* 시설 감시

1. **재고 및 자산 관리**

* 재고 추적
* 운송 프로토콜
* 운송 중 재고의 현장 보관

1. **정보기술 보안**

* 인터넷 사용 정책
* 인증 및 권한 부여
* 비밀번호 정책
* 악성 코드 방지/바이러스 백신
* 참고: 모두 포함(허용 가능한 사용 등)

1. **인사 정책 및 절차**

* 직책에 보안 포함
* 근무자 적격심사
* 기밀유지, 재산권 및 지적재산권 보호 계약
* 고용 약관
* 업무 분장(SOD)
* 고용 종료
* 징계 조치
* 보안 인식 및 교육 프로그램
* 직원 및 임시직/프리랜서의 신원/평판 조회 및 적격심사
* 직원 및 임시직/프리랜서와의 비공개 계약(NDA)
* 기록 보존

1. **제3자**

* 제3자 계약
* 비공개 계약(NDA)

1. **사고 대응**

* 사고 파악 및 분석
* 사고 상달 및 보고
* 사고 대응 절차 및 방법
* 사후 검토 절차 및 얻은 교훈

부록 G - 기타 자료 및 참고문헌

국제표준화기구(ISO), 표준 27001. *정보 기술 - 보안 기법 - 정보보호 관리체계 - 요구사항.* 2005년 10월. <http://www.27000.org/iso-27001.htm>

국제표준화기구(ISO), 표준 27002*. 정보 기술 - 보안 기법 - 정보보호 관리를 위한 행동규약.* 2007년 7월. <http://www.27000.org/iso-27002.htm>

국제표준화기구(ISO), 표준 27005. *정보 기술 - 보안 기법 - 정보보호 위험관리*. 2008년 6월.<http://www.27000.org/iso-27005.htm>

미국표준기술연구소(NIST) 특별 발행물 800-53. *연방 정보 시스템 보안 통제장치 권고안(Recommended Security Controls for Federal Information Systems)*, 2005년 2월. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

미국표준기술연구소(NIST) 특별 발행물 IR 7298. *Glossary of Key Information Security Terms,* 2006년 4월.

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

SANS(SysAdmin, Audit, Networking, and Security) 연구소. *Glossary of Terms Used in Security and Intrusion Detection*

<http://www.sans.org/resources/glossary.php#m>

OWASP(Open Web Application Security Project) – 시험 설명서

<http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf>

미국표준기술연구소(NIST) 특별 발행물 800-88. *Guidelines for Media Sanitization*, 2006년 9월. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Industrial Security Program - 운영지침서(DoD 5220.22-M), 2006년 2월

http://dtic.mil/whs/directives/corres/pdf/522022m.pdf

인터넷 보안 센터 – 보안 벤치마크 http://benchmarks.cisecurity.org/

미국국가안전보장국(NSA) - 보안 구성 설명서 https://www.nsa.gov/ia/mitigation\_guidance/security\_configuration\_guides/

미국표준기술연구소(NIST) 특별 발행물 800-92. *Guide to Computer Security Log Management,* 2006년 9월. <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

미국표준기술연구소(NIST) 특별 발행물 800-44. *Guidelines on Securing Public Web Servers,* 2007년 9월. <http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>

미국표준기술연구소(NIST) 특별 발행물 800-40. *Creating a Patch and Vulnerability Management Program,* 2005년 11월. <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

부록 H - MPAA에 저작권 침해 신고

**MPAA 온라인 저작권 침해 신고**

아래 주소를 통해 MPAA에 저작권 침해를 직접 신고할 수 있습니다.

http://www.mpaa.org/contact-us/

**MPAA 및 MPA 저작권 침해 24시간 제보 전화**

MPAA가 현지 콘텐츠 보호 당국과 협력하는 각 국가별 24시간 제보 전화 연락처가 아래 목록에 나와 있습니다.

|  |  |
| --- | --- |
| **북미 및 남미 지역** | |
| 캐나다 | (800) 363-9166 |
| 미국 | (800) 371-9884 |
| **유럽, 중동, 아프리카(EMEA) 지역** | |
| 벨기에 | +32 2 778 2711 |
| 이탈리아 | (800) 864 120 |
| 네덜란드 | (909) 747 2837 |
| 우크라이나 | +38 0 445 013829 |
| 영국 | (800) 555 111 |
| **아시아 태평양(APAC) 지역** | |
| 오스트레일리아 | +61 29997 8011 |
| 홍콩 | +65 6253-1033 |
| 말레이시아 | +65 6253-1033 |
| 뉴질랜드 | +65 6253-1033 |
| 필리핀 | +65 6253-1033 |
| 싱가포르 | +65 6253-1033 |
| 대만 | +65 6253-1033 |

모든 지역별, 국가별 콘텐츠 보호 당국에 대한 일반 연락처 정보의 전체 목록은 <http://www.mpaa.org/contact-us/>에서 확인할 수 있습니다.

**MPAA 온라인 자료**

MPAA에 대한 추가 정보는 [www.mpaa.org](http://www.mpaa.org) 웹사이트에서도 확인할 수 있습니다.

상영 중 콘텐츠를 보호하기 위한 전세계 프로그램에 대한 정보는 [www.fightfilmtheft.org](http://www.fightfilmtheft.org)에서 확인할 수 있습니다.

**문서의 끝**