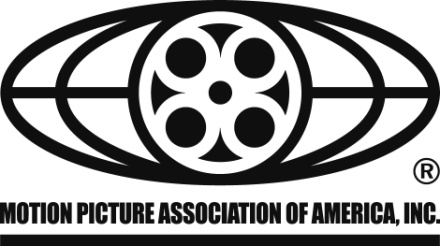
****

**美国电影协会 (MPAA) 内容安全计划**

**维护内容安全的最佳实践**

**通用指南**

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

3.0 版

2015 年 4 月 2 日

文档历史记录

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **说明** | **作者** |
| 1.0 | 2009 年 12 月 31 日 | 首次公开发布 | 德勤会计师事务所  美国电影协会 (MPAA)  美国电影协会成员公司 |
| 2.0 | 2011 年 5 月 15 日 | 更新与修订  并入通用指南与增补指南 | 普华永道律师事务所  美国电影协会  美国电影协会成员公司 |
| 2.1 | 2013 年 1 月 1 日 | 更新与修订 | 普华永道律师事务所  美国电影协会  美国电影协会成员公司 |
| 3.0 | 2015 年 4 月 2 日 | 更新与修订 | 美国电影协会  美国电影协会成员公司 |

目录

[文档历史记录 i](#_Toc427310683)

[I. 最佳实践概述 2](#_Toc427310684)

[II. 机构概述 3](#_Toc427310685)

[III. 风险管理 4](#_Toc427310686)

[IV. 最佳实践的格式 6](#_Toc427310687)

[V. 最佳实践通用指南 7](#_Toc427310688)

[附录 A — 术语表 64](#_Toc427310689)

[附录 B — MPPA 影片和发行渠道定义 67](#_Toc427310690)

[附录 C — 机构指示图 69](#_Toc427310691)

[附录 D — 控制措施的参考指示图 82](#_Toc427310692)

[附录 E — 常见问题 86](#_Toc427310693)

[附录 F— 建议的政策与程序 88](#_Toc427310694)

[附录 G — 其他资源和参考 89](#_Toc427310695)

[附录 H — 向 MPAA 举报盗版 90](#_Toc427310696)

1. 最佳实践概述

**简介**

三十多年来，美国电影协会有限公司 (MPAA) 代表其成员公司（成员）进行了内容安全测评。其成员公司包括：派拉蒙影业公司、索尼影视娱乐公司、环球影城有限责任公司、二十世纪福克斯电影公司、迪士尼电影及华纳兄弟娱乐公司

始于 2007 年，这些审查使用标准化测评模式、流程及报告模板。其后，32 个国家与地区的 500 多个机构接受了测评。

MPAA 致力于保护全球范围内为观众创造娱乐内容的公司及人员的权利。从创作型艺术到软件工业，全球范围内越来越多的人凭借其创意的力量谋生。这意味着保护知识产权以及承认这些保障措施是全球信息经济健康发展的基石，正变得越来越重要。

MPAA 内容安全计划旨在强化流程监督，保证其成员的影片内容在拍摄、后期制作、营销和发行的过程中受到保护。这是通过以下方法实现的：

* 机构服务发布一系列最佳实践，概述了标准控制措施，帮助保护成员的内容安全；
* 请第三方合作伙伴依据发布的最佳实践对内容安全进行评估；
* 加强对成员影片内容予以安全保障的重视；以及
* 提供标准的测评手段，以便成员和其商务合作伙伴就内容安全再做个人讨论。

**目的和适用范围**

本文旨在让与协会成员保持合作关系的当前和未来的第三方供应商，了解我们对一般内容安全的期望值和当前的行业最佳实践。任何成员对于供应商的选择是由其单独决定的。

制定内容安全最佳实践旨在考虑机构提供的服务，机构处理的内容类型以及机构操作的服务交付时段。

本文中概述的最佳实践受到当地、州、地区、联邦和国家法律法规的约束。

本文中概述的最佳实践，以及此处提及的产业标准或国际标准化组织 (ISO) 的参考标准会定期调整。

**对最佳实践的遵守完全出于自愿，而不作强制委派。**

**出现例外时的流程**

最佳实践不可行时，机构应记录不能实施的原因，并且实施补救措施来替代最佳实践。同时，应就出现的异常，同成员进行直接交流。

**问题或意见**

若对最佳实践有任何问题或评论，请发送电子邮件至：contentsecurity@mpaa.org

1. 机构概述

下表就提供的典型服务、处理的内容，以及每种类型机构的服务交付时段作了说明。

| **编号** | **机构类型** | **典型机构服务** | **内容类型** | **服务交付时段** |
| --- | --- | --- | --- | --- |
| **1** | **音频、配音和字幕** | * 原语和外语配音 * 字幕 * 特技音效 * 配乐 * 配音/拟音 | * 低分辨率 * 带水印的/损坏的 * 完整/部分特色内容 * 音频母版 | * 影院上映前 * 供家庭播放前 |
| **2** | **配送、交付及货运** | * 配送服务 * 交付服务 * 货运服务 | * 多样 | * 影院上映前 * 供家庭播放前 * 编录 |
| **3** | **创意广告** | * 非润色性服务 * 预告片 * 电视宣传片 * 广告传单 * 绘图 * 网络广告 | * 带水印的，损坏的完整/部分特色内容 * 剧照 * 剪辑 | * 影院上映前 * 供家庭播放前 * 编录 |
| **4** | **数字**  **电影** | * 数字电影母版制作 * 复制 * 密钥管理 | * 高清 - 完整或部分内容 * 数字电影发行母版 * 数字电影组件包 | * 影院上映前 |
| **5** | **数字**  **服务** | * 数字中间片 * 扫描 * 影片转录 * 旧片修复 | * 高清 - 完整或部分内容（胶卷） | * 影院上映前 * 编录 |
| **6** | **发行** | * 发行 * 产品履行 * 幕后/影片存库 * DVD/磁带回收 | * 高清 * 清晰影像 | * 影院上映前 * 供家庭播放前 * 编录 |
| **7** | **DVD**  **制作** | * 压缩 * 编辑制作 * 编码 * 区域分划 * 特别制作 * 碟片质保检验 | * 清晰 - 完整的正片 | * 供家庭播放前 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **机构类型** | **典型机构服务** | **内容类型** | **服务交付时段** |
| **8** | **DVD**  **制作** | * 压缩 * 编辑制作 * 编码 * 区域分划 * 特别制作 * 碟片质保检验 | * 清晰 - 完整的正片 | * 供家庭 * 播放前 |
| **9** | **机上娱乐 (IFE)和**  **接待服务** | * 机上娱乐实验室 * 机上娱乐集成 * 宾馆 * 航空公司 * 游轮/渡船 * 图书馆 * 医院 * 监狱 | * 高清 - 完整或部分内容 * 损坏的 - 完整或部分内容 | * 影院上映前 * 供家庭播放前 * 编录 |
| **10** | **后期制作服务** | * 电视电影 * 复制 * 编辑 * 后期修饰 * 质量控制 | * 高清 - 完整或部分内容 | * 影院上映前 * 供家庭播放前 * 编录 |
| **11** | **复制** | * 母版前期制作 * 母版制作 * 复制 * 校验碟制作 | * 高清 * 清晰影像 | * 供家庭播放前 |
| **12** | **视觉**  **特效**  **(VFX)** | * 数字化后期制作 * 计算机合成影像 * 动画 | * 高清-部分 * 帧数、镜头、序列、剧照 * 剧本 * 故事脚本 | * 影院上映前 * 影院上映后（2D 到 3D） |
| **13** | **应用程序** | * 应用程序开发 | * 多样 | * 多样 |
| **14** | **云端** | * 主机 * 数据中心 | * 多样 | * 多样 |

1. 风险管理

**风险评估**

通过风险评估来预测风险，并执行适当的控制程序将风险降低到可接受范围，确保商业目标的达成。

国际标准化组织 (ISO) 27000 将风险定义为“事件发生的几率和后果的结合” 例如，内容从机构网络中失窃并公开发布会有多大的几率，而如果事件发生，随之对公司及其客户又会带来何种商业后果（如合同违约和/或在服务交付时段中产生收入损失）。

ISO 27001 中强调了拥有稳健管理系统的重要性，并介绍了如何建立一个信息安全管理系统 (ISMS)。

**资产分类**

在你们的机构，进行资产分类的过程有四步，总结如下：

监控和评估有效性

确定最低限度的安全控制集

实施控制

识别和分类资产

经与成员（客户）磋商，会让一个部门负责决定客户资产应该接受的安保级别。下表给出了内容分类的一个示例：

| **分类** | **说明** | **举例** |
| --- | --- | --- |
| **高级别安保内容** | 公司认为任何资产被盗或泄露都会带来经济损失、给品牌造成负面影响或遭遇严重处罚 | * 大制作影片的内容在影院首映前被盗 * 家庭播放的内容在首次上市日之前被盗 * 母版或播放版被盗 |

与每种机构类型相关的风险，其信息亦纳入相应的增补最佳实践。

**安全控制措施**

信息技术管理协会将控制措施定义为“提供适当保障，确保达成商业目标，避免或发现并纠正不利事件的政策、程序或组织结构”。安全控制措施的选用主要取决于资产的分类，对公司的价值，以及资产泄露或被盗带来的风险。

为了降低存在的风险，我们鼓励各个公司努力对特定风险实施适当的风险控制。还应根据当前的险恶环境，对这些措施的设计和有效性进行定期评估。



**管理系统**



**组织与管理**



**物理安全**



**运输**



**机构**



**数字化内容的安全**



**基础设施**



**IV. 文档的编制**



**MS-1 行政安全意识/监管   
第 7 页**

**最佳实践根据 MPAA 的电影内容安全模板编制，为评估机构保护客户利益提供了评估框架。其包括的安全主题涉及三个领域：管理系统、物理安全和数据的安全。MPAA 电影内容安全模板的组件参照了相关的 ISO 标准 (27001-27002)、安全标准（即 NIST、CSA、ISACA 及 SANS）和行业最佳实践。**

**MS-2 风险管理  
 第 7 页**

**MS-3 安保组织   
第 8 页**

**MS-4 政策与程序  
 第 9 页**

**MS-5 事件响应  
 第 12 页**

**MS-6 业务连续性和灾难恢复   
第 14 页**

**MS-7 变更控制和配置管理   
第 15 页**

**MS-8 工作流程   
第 15 页**

**MS-9 职责划分   
第 16 页**

**MS-10 背景调查  
 第 17 页**

**MS-11 保密协议   
第 17 页**

**MS-12 第三方的使用与筛选   
第 18 页**

**PS-1 入口/出口  
 第 20 页**

**PS-2 访客进入/离开 第 21 页**

**PS-3 身份识别   
第 22 页**

**PS-4 外围安全  
 第 22 页**

**PS-5 警报器   
第 23 页**

**PS-5 授权   
第 25 页**

**PS-8 密钥   
第 26 页**

**PS-9 摄像头  
 第 28 页**

**PS-7 电子准入控制 第 25 页**

**PS-10 记录与监控   
第 29 页**

**PS-11 搜查   
第 30 页**

**资产管理**

**PS-12 库存追踪   
第 33 页**

**PS-13 库存盘点   
第 34 页**

**PS-14 空白媒介/生胶片库存跟踪   
第 35 页**

**PS-15 客户资产   
第 35 页**

**PS-16 处理   
第 36 页**

**PS-17 装运   
第 38 页**

**PS-18 接收  
 第 39 页**

**PS-19 标记   
第 40 页**

**PS-20 包装   
第 40 页**

**PS-21 运输工具   
第 41 页**

**DS-1 防火墙/广域网/外围安全   
第 42 页**

**DS-2 互联网   
第 46 页**

**DS-3 局域网/内部网络   
第 48 页**

**DS-4 无线网络   
第 51 页**

**DS-5 I/O 设备安全   
第 53 页**

**DS-6 系统安全   
第 53 页**

**DS-7 帐户管理   
第 56 页**

**DS-7.7-8.4 身份验证 第 58-60 页**

**DS-9 记录与监控  
 第 61 页**

**内容管理**

**DS-10 移动安全  
 第 63 页**

**内容传输**

**DS-11 安全技术   
第 65 页**

**DS-12 内容跟踪   
第 67 页**

**DS-13 传输系统   
第 68 页**

**DS-14 传输设备的使用方法   
第 68 页**

**DS-15 客户门户   
第 70 页**

1. 最佳实践的格式

MPAA 电影内容安全模板上列出的所有安全主题的最佳实践使用如下格式：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 管理系统 | 物理安全 | | | 数字化内容的安全 | | |
| 组织与管理 | 机构 | 资产管理 | 运输 | 基础设施 | 内容管理 | 内容传输 |

表格在每页的开头处突出显示了 MPAA 电影内容安全模板中涉及的安保领域。

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| PS-9.0 | 密钥 | **主密钥**只限发放给获授权的人员（如，所有者、机构的管理层） | * 保存一份有权使用**主密钥**的**公司人员**名单 * 定期更新名单移除某些不再需要使用**主密钥**的**公司人员** |
| PS-9.1 | 执行签入/签出程序，追踪和监测**主密钥**的分发 | * 做好记录以跟踪以下信息： * **持有每个主密钥**的**公司人员** * 签出/签入时间 * 签出原因 |

P

**词汇表**

词汇表中的术语**用黑体**突出并在附录 A 中提供解释。

**实施指南**

提供其他的考虑、可能实施的步骤与范例，以帮助公司执行最佳实践。

**最佳实践**

每个安全主题都有最佳实践的概述。

**安全主题**

每一功能区域包含一个或多个“安全主题”。每一个安全主题由一个或多个最佳实施应对解决。

**编号**

每一项最佳实践都分配有固定的参考号，形式是：XX-Y.Z，XX 表示基本领域，Y 表示安全主题，Z 表示具体的控制措施。

1. 最佳实践通用指南

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-1.0 | 行政安全意识/监管 | 建立一个信息安全管理系统，实施一个由企业所有人/高级管理层批准的信息安全控制框架。 | * 例如 ISO27001 的 ISMS 框架、NIST、CoBIT 等。 |
| MS-1.1 | 每年至少要审查信息安全管理政策和程序一次。 |  |
| MS-1.2 | 每年就保护电影内容的职责，对行政管理人员/所有人予以培训及交流一次。 |  |
| MS-1.3 | 组建信息安全管理小组，制定和审查信息安全管理政策。 |  |
| MS-2.0 | 风险管理 | 开发一个正式和记录在案的安全风险评估程序，以内容方面的工作流程和敏感性资产为重点，识别并对相关机构的内容被盗或泄露的风险予以分级排列。 | * 明确界定安全**风险评估的范围并根据需要修改** * 使用一个系统的评级方式，结合风险出现的几率、风险对商业目标/内容保护的影响及资产分类，评定风险级别。 * 有关记录在案的**工作流程**的最佳实践，请参阅 MS-6.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-2.1 | 风险管理 | 关键的工作流程若发生变化，要对该变化做好年度内部**风险评估**，评估时至少要依据 MPAA 最佳实践通用指南及适用的增补指南，评估后要记录并就识别出的风险采取行动 | * 每季度在管理人员和主要利益相关者间召开一次会议，确定并记录内容被盗或泄露的风险级别 * 根据 DS-1.8 和 DS-1.9，每季度进行一次网络漏洞扫描和外部渗透测试 * 对机构认为可能发生的内容丢失会带来的主要风险予以确定 * 执行并记录为减缓或降低已确定风险的控制措施 * 监控并评估补救措施的有效性，至少每季度实施一次风险控制 * 对安保的举措、升级和维护做好文件记录和预算 |
| MS-3.0 | 安保组织 | 确定安全关键点的联络人，正式定下内容和资产保护中的人员及其职责。 | * 就负责电影内容安全的人员分工，绘制组织图和编写工作描述 * 向信息安保人员提供与其工作职能相关的政策和流程的网络培训及实地培训。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-4.0 | 政策与程序 | 制定资产和内容安全的政策与程序，政策至少要涵盖到以下主题：   * 许可使用（如，社交网络、互联网、电话、个人设备、移动设备等） * 资产和内容分类及处理政策 * 业务连续性（备份、保留和恢复） * 更改控制和配置管理政策 * 保密政策 * 数字录制设备（如智能手机、数码相机、数码摄像机） * 应对例外情况的政策（如，记录偏离政策的过程） * 事件响应政策 * 移动设备政策 * 网络、互联网和无线网络政策 * 密码控制（如，设定密码的最小长度和屏幕保护程序） * 安全政策 * 访客政策 * 惩处/制裁政策 * 内部匿名举报内容盗版或错误处理（如，电话热线或电邮地址） | * 制定政策和程序时考虑机构/业务特定的工作流程。 * 所有政策和程序在发布与启用前要经过执行管理人员的签发 * 新人入职培训时要将惩处措施传达给员工 * 要了解政策和程序的完整列表，请参阅附录 F |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| MS-4.1 | 政策与程序 | 每年至少要审查和更新安全政策和程序一次。 | * 每年的安全政策与程序的管理审查要结合以下因素： * 最近的安全趋势 * 公司员工的反馈 * 新的险情和漏洞 * 监管机构（如联邦贸易委员会 (FTC) 等）的建议 * 既往安全事件 |
| MS-4.2 | 所有现行政策、程序和/或客户规定及其它更新文件均传达及要求所有的**公司员工**（如，职员、临时工和实习生）以及**第三方员工**（承包商、自由职业者和临时机构）员工签字。 | * 向新**公司员工**和**第三方员工**分发涵括所有一般政策与程序在内的公司手册 * 向**公司员工**和**第三方员工**通知安全政策、程序及客户规定的最新修订内容 * 管理人员必须保留所有**公司员工**和**第三方员工**签字的现行政策、程序和客户规定。 |
| MS-4.3 | 政策与程序 | 制定和定期更新关于安全政策和程序的意识计划，并在雇佣时及之后的每年向**公司员工**和**第三方员工**培训这些安全政策和程序，至少要涵盖到以下主题：   * IT 安全政策和程序 * 内容/资产安全和一般处理以及客户的特定规定 * 安全事件报告和上报 * 惩处政策 * 向所有处理加密内容的人员传授加密和密匙管理 * 资产处置和销毁流程 | * 在管理人员/员工会议上传达安全意识信息 * 实施追踪程序，追踪已完成其年度安全培训的**公司员工**（例如，数据库仓库、出勤记录、结业证书） * 提供网上或面授培训，向**公司员工**和**第三方员工**讲解常见事件、相应风险以及报告已发现事件的责任 * 分发安全意识材料（例如海报、电邮或期刊），以增进安全意识 * 根据与敏感内容有关的工作职责及交互（例如，IT 人员、产品）制定定制消息和培训，以缓和盗版问题 * 考虑记录培训课程，并提供记录以供参考 |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-5.0 | 事件响应 | 建立一个正式的事件响应计划，对发现和上报安全事件后要采取的行动作出说明 | * 在**事件响应**计划中考虑加入以下部分： * 事件的定义 * 通知安保小组 * 加大管理力度 * 分析产生的影响与优先处理事项 * 遏制影响的扩大 * 根除和恢复 * 主要联系人信息，包括客户制作室的联系信息 * 通知受影响业务合作伙伴和客户 * 执法通知 * 事件详情报告 * 有关计算机安全事件处理，请参阅 NIST SP800-61 版本 2 |
| MS-5.1 | 成立安全事件响应小组，负责发现、分析、补救安全事件。 | * 纳入不同务部门的代表以处理不同种类的安全事件；要考虑以下方面： * 管理 * 物理安全 * 信息安全 * 网络小组 * 人力资源 * 法律 * 为**事件响应**小组提供培训，以便小组成员明白其在处理事件时的角色和责任 |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-5.2 | 事件响应 | 制定安全事件上报程序，便于个人把发现的安全事件汇报给安全**事件响应**小组 | * 考虑开通匿名热线或网站，用于上报不当及/或可疑活动 * 考虑实施用于上报事件的集团电子邮件地址，以通知事件响应小组的全体成员 * 考虑采用 MPAA 举报热线以便匿名举报可疑活动 - 请参阅附录 H 中的 24 小时举报热线联系信息 |
| MS-5.3 | 若客户的内容有可能已泄露、被盗或出现其它险情（例如，丢失的客户资产），应立即通报给客户，并与管理人员和客户举行事后剖析会议。 | * 执行违反安全事项时的通知程序，包括使用通知违反安全事项的表格 * 请法务组来判定该采取何种合理的措施向相关客户通报内容丢失事件 * 讨论从事件中得到的教训，改进事件响应计划和流程 * 进行根源分析，确定未能阻止该事件发生的安保缺陷 * 修改安保控制措施防止类似事件再度发生 * 与事件波及到的客户沟通事后剖析结果，包括正确的处理方案 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| MS-6.0 | 业务连续性和灾难恢复 | 制定正式计划，说明须采取的行动，以便确保业务连续性。 | * 考虑将下列部分纳入**业务连续性**计划： * 对关键资产和内容的威胁，包括失去电力和通讯、系统故障、自然灾害等 * 详细的信息系统、内容和元数据备份程序及系统信息文档，包括关键的 WAN 和 LAN 配置/内部网络设备 * 备份加密（至少 AES-128 位加密） * 至少可为闭路电视系统、警报器、关键信息系统（包括执行关键系统安全停机的软件）供电 15 分钟的备用电源 * 考虑使用异地备份位置 * 通知安保小组 * 加大管理力度 * 分析产生的影响与优先处理事项 * 遏制影响的扩大 * 恢复的优先次序和详细的恢复程序，包括恢复系统的手动变通方法和配置详情 * 主要联系人信息 * 通知受影响业务合作伙伴和客户 * 每年至少测试业务连续性和灾难恢复程序一次 |
| MS-6.1 | 成立业务连续性小组，负责发现、分析、补救连续性事件。 | * 纳入界定的角色和责任 * 为业务连续性小组提供培训，以便小组成员明白其在处理事件时的角色和责任 |
| MS-7.0 | 变更控制和配置管理 | 制定政策和程序，以确保新数据、应用程序、网络和系统组织得到企业领导的批准。 | * 纳入介绍设备、服务和功能的安装、配置及使用的文件，需要时纳入更新文件 * 制订处理已知问题的政策和程序 * 纳入上报错误和安全缺陷的政策和程序 * 限制和监控安装未经授权的硬件或软件 * 管理与数据、应用程序、网络基础设施和系统变更有关的风险 * 记录和保留所有变更请求、测试结果和管理人员批准 |
| MS-8.0 | 工作流程 | 制订**工作流程**跟踪内容和授权检验点。纳入下列关于物理和数字内容的过程：   * 交付（接收/退还） * 接收 * 转移 * 储存 * 删除/销毁 | * 使用泳道图制订**工作流程** * 包括适用时对资产进行加工与处理的信息 * 评估每个接触点，衡量对内容造成的风险 * 实施检验点的授权控制 * 制定相关应用程序控制措施 |
| MS-8.1 | 程序发生变更时更新**工作流程**，每年至少审查**工作流程**过程一次。 | * 在各个过程中遵循内容**工作流程**并实施控制措施，以发现存在漏洞的领域 |
| MS-9.0 | 职责划分 | 划分内容**工作流程**中的职责。如果划分职责是不切实际的，要实施和制订补偿控制措施。 | * 要以文件形式定下人员与职责，避免不同人员在职责上有重叠，比如： * **仓库**和服务器/机房人员 * 装运与接收人员 * 资产从**仓库**和内容/制作区域向机构内部（例如，操作人员）转移 * **数字资产**文件夹访问权限（如，数据管控人员为制作人设置数据访问权限） * 从制作人员到内容传输人员 * 使用人力控制（如，处理电影内容前申请得到制作人的批准）或使用工作分配系统的自动化控制（如，**工作流程**的不同阶段都要得到自动化审批）来划分责任 * 当职责划分难以做到时，实施其他的补偿性控制措施，如： * 监控公司员工和/或第三方员工的活动 * 保留并审查审计记录 * 实施实体分离 * 实施管理人员监督 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| MS-10.0 | 背景调查 | 对所有**公司员工**和**第三方员工**进行背景审核调查。 | * 依据相关法律、法规、工会章程和文化因素进行背景调查 * 运用背景审核调查筛选潜在的**公司员工**和**第三方员工**，这些程序要与公司要求、员工所接触之内容的敏感性、内容失窃和泄露的风险几率相称 * 必要时，进行身份、学历和专业资格的审查。 * 如果背景调查不符合法律规定，则记录为例外情况，使用征信调查 |
| MS-11.0 | 保密协议 | 要求所有**公司员工**在雇佣时和之后的每年，签署一份保密协议（比如，不披露内容），包括处理和保护内容的要求。 | * 纳入在他们受雇、签约或协议期满后，仍需进行保密的不披露指南 * 必要时，解释非法定保密情况下的保密/不披露协议的重要性 * 确保**公司员工**用来处理商业敏感内容之设备上的所有相关信息都移交给公司，并且安全地从设备上移除 * 管理人员必须保留所有**公司员工**签署的保密协议 |
| MS-11.1 | 要求所有**公司员工**在雇佣期或签约期满时，返还他们掌握的所有内容和客户信息 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-12.0 | 第三方的使用与筛选 | 要求处理内容的所有**第三方员工**（例如，自由职业者）在雇用时签署保密协议（比如，不披露内容）。 | * 纳入在他们受雇、签约或协议期间或期满后，仍需执行保密相关政策的不披露指南 * 必要时，解释非法定保密情况下的保密/不披露协议的重要性 * 确保**第三方员工**用来处理商业敏感内容之设备上的所有相关信息都移交给公司，并且安全地从设备上移除 * 管理人员必须保留所有**第三方员工**签署的保密协议 * 纳入处理和保护内容的要求 |
| MS-12.1 | 要求所有**第三方员工**，在签约期满时，返还他们掌握的所有内容和客户信息 |  |
| MS-12.2 | 纳入第三方合同中的安全要求。 | * 要求**第三方员工**遵守第三方合同中规定的安全要求和客户要求 * 纳入涉及敏感性内容之活动的审计权限条款 * 执行程序，监控安全要求的遵守情况 |
| MS-12.3 | 实施一项程序，以便在结束雇佣关系时收回**内容**。 | * 确保第三方设备上的所有**内容**都移交给公司，并且安全地从设备上移除 |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| MS-12.4 | 第三方的使用与筛选 | 要求**第三方员工**在适当的时候（如提供快递服务时）都有保价及已投保。 | * 要求**第三方员工**提供保险证明，并记录下保险公司和保单号码 * 要求第三方的保险达到一定的承保范围 * 续约时，需要每年更新信息 |
| MS-12.5 | 除非工作职能所需，否则严格控制第三方进入内容/制作区域。 | * 确保不向**第三方员工**提供进入存放内容区域的电子权限 * **第三方员工**（如清洁工）需要进入限制区域（如**仓库**）时，需有人陪同 |
| MS-12.6 | 如果使用**分包商**处理内容或将工作转包给另一家公司，须通知客户。 | * 要求客户书面签字/批准 * 要求分包商完成标准的**尽职调查**活动 * 将工作转包给另一家公司必须上报 MPAA 成员制作室，且必须完成 MPAA 供应商问卷调查并提交给成员制作室以作尽职调查。 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| PS-1.0 | 入口/出口 | 确保机构的所有入口/出口始终上锁，包括装货区的门窗。 | * 如果机构的接待区域和配备门禁的其他区域是隔离开的，允许进/出口在上班时间不上锁 |
| PS-1.1 | 通过隔离内容处理区域和其他机构区域（如办公室、等候室、装卸区、速递员收件和送件区、复制和母版制作室），实施电影内容处理区域的进出控制。 | * 在理解进出须知后方允许进入内容/制作区 * 要求对用于放映的房间实施门禁控制（如放映室） * 有限度地控制进入**放置媒体**播放器（如蓝光光碟、DVD）的房间 * 执行职责划分模式，以此限制任何一人同时进入复制和母版制作室 |
| PS-1.2 | 在有两种业务并存的机构中实施门禁控制，包括但不限于：   * 划分工作区域 * 对可区分业务单位的入口和出口实施门禁控制 * 记录和监控机构内的所有入口和出口 * 机构内的所有员工在雇佣前必须向客户报告 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| PS-2.0 | 访客进入/离开 | 维护好访客的详细日志，包括以下内容：   * 姓名 * 公司 * 进入时间/离开时间 * 受访人员 * 访客签字 * 分发的卡号码 | * 要求所有访客出示有效的带照片证件（如驾照或政府发行的身分证明），用以核实其身份 * 建议隐藏之前访客的姓名 |
| PS-2.1 | 给每位访客分发**一个身份识别卡**或身份识别便签，要求其始终佩带，并在其离开时收回。 | * 访客的识别卡需要能轻易与**公司员工**的识别卡（如塑料色码卡）进行区分 * 建议每日轮用不同的纸质卡或便签颜色 * 建议使用有效期满时会改变颜色的卡 * 在进入/离开时记录卡的分发与返还 * 访客的识别卡应当按次序编号，以供追踪 * 每日对卡予以计数 |
| PS-2.2 | 不要给访客提供进入内容/制作区的钥匙卡 |  |
| PS-2.3 | 要求访客由现场的授权员工或至少由内容/制作区的授权员工陪同 |  |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| PS-3.0 | 身份识别 | 给**公司员工**和长期的**第三方员工**（如房屋维护清理人员）配备带照片的**身份识别卡**，并要求全时佩戴。 | * 在背景调查结束之后，给所有**公司员工**和长期的**第三方员工**发放带照片的**身份识别卡** * 建立和执行一个在合同期满后立即回收员工带照片**身份识别卡**的程序 * 建议在带照片**身份识别卡**上忽略住址、公司名称、标识和其他特定信息 * 可能的话，建议把**带照片身份识别卡**当做出入钥匙卡 * 要求员工在**带照片身份识别卡**丢失或失窃后立即上报 * 提供一个 24/ 7 服务的电话号码或网站用以报告**带照片身份识别卡**的丢失或失窃 * 培训和鼓励员工质疑未佩戴可见身份证的人员 |
| PS-4.0 | 外围安全 | 执行外围安全措施，以应对**风险评估**中组织所确定的、可能由机构来承受的风险。 | * 基于机构的位置和布局执行外围安全措施，比如： * 通过使用墙壁、围栏和/或大门限制进入机构的外围，至少也要在下班后启用保护；墙壁/围栏应当至少 8 英尺高 * 必要时，保护和封锁公共外域，比如吸烟区和露台 * 在公共外部区域（如吸烟区）和停车场安置足够的外置摄像头 * 请认识到过度使用公司引导标示可能招致定标侵入 * 必要时，在外围使用报警器 |
| PS-4.1 | 在外围入口和非应急进出口设置保安。 |  |
| PS-4.2 | 外围安全 | 按照一份随机的时间表，每天进行安全巡查并且在日志里记录巡查的结果。 | * 要求保安巡查内部和外部区域 * 包括检查紧急出口，同时核查密封情况 * 考虑使用电子安保巡查系统来追踪巡查（例如，检查站点）并且检查上锁情况 |
| PS-4.3 | 始终锁上外围大门。 | * 设置电子起降杆，由保安负责，以控制车辆进入机构 * 给公司的员工和填妥适当文书的第三方工作人员分发停车证 * 要求访客车辆出示证件，并保证所有的访客都取得了预先授权方可进入该厂区 |
| PS-5.0 | 警报器 | 安装集中声音报警系统，覆盖所有进出口（包括应急出口）、窗户、装载区、消防通道及禁入区（如**仓库**、服务器/机房等）。 | * 在每个入口安装警报器，提醒安保人员注意未经授权进入设备区的行为 * 当机构无人监督时，启用警报器 |
| PS-5.1 | 在禁入区（例如，**仓库**、服务器/机房）安装及有效安置动作感应器，并有效配置它们，以警告适当的安保及其他人员（例如，项目经理、制片人、编辑主管、事件响应团队等）。 | * 确保警报系统在正常工作时间之后能够覆盖存储区域和**仓库**（如通过动作感应器），作为附加的保险措施 |
| PS-5.2 | 在禁入区（例如，仓库、服务器、机房）的门边上安装警报器，便于在敏感的进出口开启时间长于先前设定的时间（如 60 秒）时，发出警报通知。 | * 安装控制出入的门，当门的开启时间长于设定的时长时，引发警报，提醒安保人员 |
| PS-5.3 | 警报器 | 安装警报器直接向负责安保的人员及其他人员（例如，项目经理、制片人、编辑主管、事件响应团队等）提供警告通知。 | * 如果通知之后，未从安保人员那收到及时回复，则启用和实行升级步骤 * 发生违规行为，建议执行自动执法通知 * 在周末和下班之后，执行通知程序 |
| PS-5.4 | 给每位需要进入报警系统的人员分发独特的启用代码和解除代码，严格限制其他人进入报警系统。 | * 使用独特报警代码追踪负责启用/解除报警器的安保人员 * 在管理人员准许的时间间隔内更新分发的报警代码，降低分享和丢失代码的风险 |
| PS-5.5 | 每季度或人员变更后复审可启用和解除报警系统的用户名单。 | * 移除离开公司或换了工作岗位的用户 * 停用已移除用户的报警代码 |
| PS-5.6 | 每季度测试报警系统一次。 | * 演练违反物理安全的行为，确保下列操作： * 报警系统发现违反行为 * 安保人员收到警报 * 根据步骤，安保人员及时做出反应 |
| PS-5.7 | 实施安全措施，以便在断电、消防门无法开启、和其他所有门关闭失败的情况下，避免未经授权进入。 |  |
| PS-6.0 | 授权 | 记录并执行程序，以管理机构的准入权并记录**准入权**的任何变动。 | * 指定一名员工负责机构的准入权 * 通知相关人员（如机构管理人员）员工身份的变化 * 制作一分纸质表格或电子表格，表格必须由主管填写，以便**公司员工**和/或**第三方员工**提交机构准入请求 * 就审查和批准机构准入请求分派职责 |
| PS-6.1 | 只允许指定人员进入制作系统。 |  |
| PS-6.2 | 在每季度及当**公司员工**和/或**第三方员工的**职位或雇佣状态有变动时，复审进入禁入区（如**仓库**、服务器/机房）的准入权。 | * 验证公司职工与第三方工作人员的身份状态 * 移除终止的用户的准入权 * 确认准入权与使用者的相关工作职能相符 |
| PS-7.0 | 电子准入控制 | 对整个公司机构实行电子准入，覆盖所有进出口和所有存储、传输或处理内容的区域。 | * 根据工作职能和责任，分发具体机构区域的电子准入权 * 根据公司员工和第三方员工职位的变化或终止，更新电子准入权 * 保留记录公司人员电子准入设备号码的日志 * 查看记录和监控 PS-10.0 * 对公共区域（如公用电梯）不需要使用电子准入权的时间进行审核 |
| PS-7.1 | 电子准入控制 | 只有合适人员拥有电子准入系统的管理权。 | * 只有指定的人员拥有电子系统管理权，不允许制作内容的个人参与到电子准入的事务中 * 指派一个独立小组管理和控制电子准入系统 |
| PS-7.2 | 在上锁的柜子中存放卡片纸和**电子访问设备**（例如，钥匙卡、密匙卡），并确保**电子准入设备**在分配予人员前保持未启用的状态。在上锁的柜子中存放未被分配的电子准入设备（例如，钥匙卡、密匙卡），并确保其在分配予人员前保持未启用的状态。 | * 只有**钥匙卡**/**电子准入设备**系统管理小组有权接近上锁的柜子 * 存货出库需作签出记录 |
| PS-7.3 | 在系统中禁用丢失的**电子准入**设备（例如，钥匙卡、密匙卡），方可发出新的**电子准入设备**。 | * 教育**公司员工**和**第三方员工**应立即上报**电子准入设备**的丢失，防止未授权进入机构的行为发生 * 发出替换**电子准入设备**前要求识别身份 |
| PS-7.4 | 根据规定的时间表，发出设有到期日期（如 90 天）的第三方**电子准入设备**。 | * 确保可轻易辨认第三**方电子准入设备**与**公司员工**电子准入设备 * 确保**电子准入设备**上的截止日期很容易辨认 * 在第三**方**理解进出须知后向其发放电子准入设备 |
| PS-8.0 | 密钥 | 禁入区的**主密钥**和/或钥匙只限发放给获授权的人员（如，所有者、机构的管理人员）。 | * 保存一份有权使用**主密钥**的**公司人员**名单 * 定期更新名单移除某些不再需要使用**主密钥**的**公司人员** |
| PS-8.1 | 执行签入/签出程序，追踪和监测禁入区的**主密钥**和/或钥匙的分发。 | * 做好记录以跟踪以下信息： * 持有每个主密钥的**公司人员** * 签出/签入时间 * 签出原因 * 在规定时间内要求归还**主密钥**，如没及时归还，调查密钥在谁手中 |
| PS-8.2 | 在外部进出口，只能使用由特定的锁匠配制的钥匙。 | * 使用安全级别高的钥匙（圆筒型），提供更高安全级别，防止出现以下两种或以上情况： * 撬开 * 压印 * 复制钥匙 * 钻孔 * 其他形式的强力侵入 |
| PS-8.3 | 每季度点验开启禁入区（包括机构的入口/出口）的**主密钥**和钥匙。 | * 确认、调查和处理任何丢失钥匙的事件（丢失/遭窃） * 检查记录日志，查看最后以钥匙签出但未能说明原因的人员 * 若开启禁入区的**主密钥**或钥匙丢失而未能说明原因，更换门锁 |
| PS-8.4 | 取得终止的员工/第三方或不再需要准入权之人士的所有钥匙。 |  |
| PS-8.5 | 密钥 | 若主密匙或副密匙丢失或遗失，对整个机构执行电子准入控制或更新密匙。 |  |
| PS-9.0 | 摄像头 | 安装**闭路电视**系统，监控记录发生在所有的机构进出口和禁入区（例如，服务器/机房）的情况。 | * 摄像头电缆和电线须谨慎地隐藏在看不见及按理无法接触到的地方 * 机构不应假定楼内已安放充足的闭路电视 * 在机构的每个入口安放摄像头 * 确保摄像头覆盖到存储区和**仓库** |
| PS-9.1 | 至少每天检查一次摄像头的位置和记录，以确保监控录像有充分的覆盖范围、功能、影像质量、照明条件、帧速率。 | * 检查摄像头位置，确保所有进出口和其他敏感区域的视野没有遮掩 * 安装适于暗区域使用的摄像头（如弱光或红外线摄像头、动作侦测灯） * 检查影像质量，确保照明充足、人物面部可辨认 * 检查帧速率，确保录像能充分捕捉到活动 * 调整摄像头位置，避免捕捉到展示中的影片内容 * 确保录像有足够的分辨率，以便识别面部特征 * 至少以每秒 7 帧的速率录像 |
| PS-9.2 | 只有负责管理/监控系统的人员有权对**闭路电视控制台**和**闭路电视**设备（如数码录像机）进行物理接触和逻辑接触。 | * 将闭路电视**设备放置**在安全位置，对准控制进出的所在（如计算机房、上锁的柜子、箱子） * 对准入权进行周期性检查，确保只有合适的人员能接触到监控设备 * 确保基于 IP **的闭路电视**系统的网络控制台仅限于授权人员使用，保证稳固的帐户管理控制措施就位（如密码的复杂性、个人用户登录、记录与监控） |
| PS-9.3 | 摄像头 | 在安全位置，保证监控影像包含准确的日期和时间戳，并保证**闭路电视**的监控影像和电子进入记录保留至少 90 天，或者保留到法律规定的最长时限。 | * 将时间和日期刻录到实体**媒体**上，以便摄下的影像记录到磁带和光盘上 * 确保准确的时间戳保存到摄下影像的记录设备上 * 至少每周检查一次日期和时间戳的准确性 * 建议把记录内容储存在进出受控的柜子或计算机房 * 确定需要持续一天记录的典型空间大小，确保日志文件的大小足够记录至少 90 天的内容，或者至法律规定下的最大保存期 * 建议保留闭路电视监控影像到首次制作发行日期 |
| PS-9.4 | 委派一名员工或一组员工在工作时间负责监控录像，如果发现安全事件，应立即展开调查。 | * 整合事件响应程序以便处理安全事件 * 建议在接待处或 IT 办公室添加监视监控器。 |
| PS-10.0 | 记录与监控 | 至少每周记录并检查一次禁入区的电子准入权，监测可疑事件。 | * 确认并记录一系列可疑事件 * 考虑执行自动报告程序，当发现可疑的电子准入行为时，给相应的安保人员发送即时警报 * 至少将记录保留一年 * 记录并检查下列事件： * 多次尝试进入失败 * 异常时间进入 * 依次进入多个区域 |
| PS-10.1 | 记录与监控 | 至少每天记录和检查下列区域的电子准入权：   * 母版/压模库 * 母版前期制作 * 服务器/机房 * 废料间 * 高安保货笼 | * 确认并记录认为可能属异常的事件 * 考虑执行自动报告程序，当发现可疑的电子准入行为时，给相应的安保人员发送即时警报。 |
| PS-10.2 | 调查检测到的可疑电子进入活动。 | * 确认并与主要的联系人沟通，在发现异常的电子进入活动时应通知这些联系人 * 建立并执行升级程序，在主要联系人没有及时回应事件通知的情况下执行 |
| PS-10.3 | 不间断记录所有确认的电子进入事件，包括记录后续的活动。 | * 通过**事件响应**的报告表记录确认的**钥匙卡/电子准入设备**事件 * 定期检查所有最近发生的**钥匙卡/电子准入设备**事件，分析根本原因，鉴定漏洞，并适当修补 |
| PS-11.0 | 搜查 | 在当地法律允许的范围内制定政策，让保安随机搜查个人、包包、包裹和个人物品是否装有客户内容。 | * 向所有**公司员工**和**第三方员工**传达有关的搜查政策 * 对**公司员工**和**第三方员工**执行定期搜查，验证政策的执行效果 |
| PS-11.1 | 搜查 | 实施出口处搜查程序，这适用于机构的所有工作人员和访客，包括：   * 脱掉外套、帽子、皮带，进行检查 * 掏出口袋里的所有物品 * 在保安监督下，进行自我检查 * 仔细检查所有的包 * 检查笔记本的 CD/DVD 托盘 * 使用手持式金属探测器在三英寸之内对人员进行扫描搜查 | * 指导保安搜寻禁止带进现场的物品（例如，摄像机）或者没有授权文件不允许带出现场的胶片材料 * 把在出口处进行搜查的政策通知给全体公司员工和第三方工作人员 * 错开交接班的时间，防止队伍太长，延长等待时间 |
| PS-11.2 | 禁止工作人员进出公司时，携带数字录制设备（例如，**USB** 快闪存储器、数码摄像机、手机），同时这些设备也包含在出口处搜查的范围之内。 | * 没收在检查中发现的任何数字录制设备并将其存放在安全的储物柜里 * 记录任何企图窃取电影内容的事件 * 对于企图窃取电影内容的人员，采取必要的惩处措施 * 实行政策，禁止携带具有数字录制功能的移动/蜂窝技术设备 * 如果贴了明显的防拆封标签，则允许携带具有数字录制功能的手机进出 |
| PS-11.3 | 对于任何带入制作区的食物，都要使用透明塑料袋和饭盒。 | * 考虑在制作区以外划定一个进餐区域 |
| PS-11.4 | 实行着装规范政策，禁止穿过大过肥的服装（例如，肥大的裤子、超大连帽运动衫）。 |  |
| PS-11.5 | 使用编号、防拆封标签/全息图来辨识授权允许带进带出机构的设备。 |  |
| PS-11.6 | 搜查 | 实施程序来测试出口搜查手续。 | * 定期审核搜查的程序，确保保安搜查彻底 * 确定完善出口搜查程序的办法 * 记录搜查程序的所有审核结果和获得的改进 |
| PS-11.7 | 在车辆离开机构的停车场时，进行随机搜查。 |  |
| PS-11.8 | 隔离制作高度敏感内容的复制生产线，并且要在该隔离区域的出口实施搜查。 |  |
| PS-11.9 | 采取额外的控制措施来监督保安的行为。 | * 保安在离岗时，审查出口搜查程序 * 对保安监管工厂/制作区域和出口的职责（例如，搜查流程）予以划分 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| PS-12.0 | 库存追踪 | 执行一个内容资产管理系统，提供实体资产（即客户提供的在机构创建的资产）的详细追踪信息。 | * 要求提供授权协议书或工作定单，确认内容能由指定的个人检验 * 要求个人展示身份验证证明 * 要求对所有资产贴标签（如条形码、唯一身分证明） * 记录所有签入/签出的资产 * 记录签出资产的预计持续时间 * 建议使用自动报警器，如未于营业日或授权时间段结束退回资产，则发出资产警报通知。 * 追踪签出但未偿还资产的个人 * 记录每项资产的具体位置 * 记录每笔交易的日期和时间 |
| PS-12.1 | 用条形码标识客户资产，在收到收据时制作媒体（如磁带、硬盘驱动器），资产不使用时，存储在仓库。 | * 使用双条形码追踪资产（如在资产上和包装盒上都贴有条形码） * 在标上条形码后直接将资产送入**仓库**，在不需要使用时，也要立即返还到**仓库**中 |
| PS-12.2 | 至少将资产流动的交易记录日志保存一年。 | * 保存所有资产流动的纸质记录或数字化记录；记录内容包括： * 签入/签出资产的条形码或唯一身分证明 * 签入/签出的日期和时间 * 签出资产人员的姓名和唯一身分证明 * 签出原因 * 资产位置 |
| PS-12.3 | 库存追踪 | 至少每周检查一次电影内容**资产管理**系统的记录并且调查异常情况。 | * 确定没有在预计归还日期之前归还的资产 * 追踪到最后签出丢失资产的个人 * 对不遵守**资产管理**政策的人员实施惩处措施 * 当签出资产没有按时归还时，建议实行自动通知 |
| PS-12.4 | 使用资产跟踪系统和实体资产时，使用制作室的化名（如适用）。 | * 建议适当时移除实体资产上的制作室名称 |
| PS-12.5 | 实施和检查每日时效报告，确定**仓库**中已签出但未签回的高度敏感性资产。 | * 通过手动或**资产管理**系统编制每日时效报告 * 调查所有的异常情况 |
| PS-12.6 | 对因不能按时送达而延迟递送或退还的资产进行上锁并登记。 | * 制订在出入受控的区域中储存资产的程序 * 保留记录资产现场存储的文件，包括储存的时间和原因 |
| PS-13.0 | 库存盘点 | 客户的各项资产进行每季度库存盘点，按**资产管理**记录进行调整，并立即就其中的变动与客户沟通。 |  |
| PS-13.1 | 把负责**仓库**的员工和执行库存盘点的员工的职责进行分离。 | * 指派不在**仓库**工作的员工对计数结果进行随机抽查 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| PS-14.0 | 空白媒介/生胶片库存跟踪 | 收到空白媒介/生胶片时，给每个都贴上标签（如贴上条形码、分发唯一识别符）。 | * 除非用来制作，否则安全的制作区域不允许出现空白或生**媒介**胶片 |
| PS-14.1 | 建立程序，每月跟踪原材料（例如，聚碳酸脂）的消耗情况。 | * 按工作定单调剂现有的生胶片使用情况，以确认库存变化 * 设置一个变化临界值，如果超出，就会启动**事件响应**程序 * 考虑把生胶片实物盘点的实施作为每月库存跟踪过程的一部分 |
| PS-14.2 | 把空白的**媒介**/生胶片存放在安全的地方。 | * 要求实施准入控制措施（如上锁的柜子、保险箱），预防无授权人员进入 * 只有负责输出创作的人员才能使用空白**媒介**/生胶片 * 个人在签出空白**媒介**/生胶片时，要求其出示合适的工作定单要求 |
| PS-15.0 | 客户资产 | 只有负责追踪和管理资产的员工才有权接触完工的客户资产。 | * 只有**负责仓库**的员工在收到有效工作定单请求的情况下，才能批准签出客户资产 * 划分职责，确保**仓库**员工不能接触加工用的制作数据 |
| PS-15.1 | 将客户资产放置在受限的安全区域（如**仓库**、保险箱或其他安全存放地点）。 | * 在**仓库**安置附加的保险箱或高安保货笼，用来存储高度敏感的内容 * 用螺栓将保险箱固定在墙体或地板结构上，保证保险箱的安全 |
| PS-15.2 | 下班后若要对高度敏感区域（例如，保险箱、高安保货笼）解锁，则需要两位**公司员工**使用各自的工作卡一同开锁。 |  |
| PS-15.3 | 客户资产 | 如果已装好但未交付的资产需要整夜存放在机构里，则使用上锁、耐火的保险箱储存。 | * 把保险箱用螺栓固定在不会移动的表面上（例如，地面、墙壁），保证保险箱的安全 |
| PS-15.4 | 安排一个专门的安全区域（例如，安全货笼、安全房间）储存未交付的播放版影片，这一区域必须上锁，控制出入并且使用摄像头和/或保安进行监视。 | * 只限有工作任务的人员才能进入 * 确保播放版影片的储藏区域完全密封、上锁并始终处于监控之中 * 实施程序，定期审查监控录像 |
| PS-16.0 | 处理 | 要求在处理前，对包含客户资产的退回的、受损的、过期的存货进行内容抹除、消磁、切碎或物理销毁。 | * 执行库存清查、账货对齐的程序，然后安全地循环使用或销毁不合格的、受损的、过期的存货 * 放到垃圾桶前，不可挽回地销毁媒介 * 建议参照美国国防部 5220.22-M 的数字粉碎和消磁标准（参见附录 G） |
| PS-16.1 | 将用来循环使用/销毁的元件保存在安全区域/容器里，防止在处理之前复制和滥用资产。 | * 制定和实施政策，在循环使用/摧毁之前，限制不合格的、损毁的、过期的存货的储存时间（如，30 天） * 在循环使用/摧毁之前，将高度敏感性资产放置在安全区域内（如**仓库**、保险箱） * 确保处理箱上锁 |
| PS-16.2 | 将资产处理日志至少保存 12 个月。 | * 将资产处理记录整合到**资产管理**程序中 * 在处理日志中纳入对所处理资产的最后处理记录 |
| PS-16.3 | 处理 | 必须现场进行销毁。必须由两位公司员工监督并签核现场销毁。如果聘请第三方公司销毁，则必须由两位公司员工监督并签核现场销毁，且必须保留销毁证明书。 | * 建议要求在证明书上提供以下信息： * 销毁日期 * 销毁/处理的资产说明 * 销毁方法 * 执行销毁资产的个人姓名 |
| PS-16.4 | 运用自动化设备将不合格的盘片从刻录设备上直接传送到废料箱里（无需人员操作）。 | * 自动化处理不奏效时，划分职责（例如，检验碟片与销毁碟片使用不同的工作人员） * 处理盘片时，保持一个记录日期和时间的签名日志 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| PS-17.0 | 装运 | 要求机构出具一份有效的工作定单/货运单，以授权在机构之外运送客户资产。 | * 在工作定单/货运单中纳入以下信息： * 工作定单/货运单的号码 * 提货人姓名及其所在公司 * 提货日期和时间 * 机构联系方式 * 制定一份表格，记录采用非常规手段运输的外送资产 |
| PS-17.1 | 追踪和记录客户资产运送细节，至少包含以下内容：   * 装运时间 * 发货人姓名和签名 * 接收者姓名 * 目的地地址 * 送递公司提供的追踪号码 * 参考相应的工作定单 | * 要求接收者签名 * 运送记录至少保留一年 |
| PS-17.2 | 确保等待领取的客户资产的安全。 | * 无人看管时，将货运和接收区域的门窗都上锁 * 资产必须上锁，直到移交给供应商/速递员 |
| PS-17.3 | 根据有效的工作定单/货运单，对离开机构的客户资产进行核验。 | * 要求速递员和送货员提供有效的身份证明，以证实其是按相应的工作定单接收货件 * 确认货运量与货运单据相符 * 运输的物品若如有任何不符或损坏，立即回报 |
| PS-17.4 | 装运 | 禁止速递员和送货员进入机构的内容/制作区。 | * 如进入内容/制作区属必要，需要有人陪同送货人员 |
| PS-17.5 | 保留单独的日志，记录运货司机的信息。 | * 保存好这份包含所有运货司机信息的日志，记录的信息包括： * 姓名 * 牵引车和拖车的牌照 * 所属公司 * 提货日期和时间 * 处理的内容 |
| PS-17.6 | 如在现场进行装运，装运前则须观察并监督打包与封装。 | * 当装载和密封拖车时，要求保安始终在场 |
| PS-17.7 | 记录、监督并审查在机构之间来回运货的行程时间、路线和交付装运的时间。 | * 建立普通运输点之间交付时间的基准并监测真正的时间，对比差异 * 对主要差异进行调查、报告并逐级上报到适当的负责人 * 指定使用获准的休息点 * 建议安装实时 GPS 跟踪系统，对意外的延误进行监控和发出警报。 |
| PS-17.8 | 除客户制作室批准的目的外，禁止以其他目的转移电影资料。 |  |
| PS-17.9 | 分批次运送影院正式上映前播放的影片（例如，分不同批次运输奇数与偶数卷）。 |  |
| PS-18.0 | 接收 | 在收货时，检查送达的客户资产，并与货运单据（如包装标签、清单记录）进行比对。 | * 确认并记录任何与单据不符之处（如遗漏物件、受损的**媒体**） * 立即将问题上报管理人员、客户和/或发货人 |
| PS-18.1 | 接收 | 确认收货记录由指定员工在收货时填写。 | * 记录以下信息： * 速递员/送货人的姓名和签名 * 收货人的姓名和签名 * 收货日期和时间 * 接收资产的详细信息 |
| PS-18.2 | 立即执行以下行为：   * 给接收的资产贴上标签（如贴上条形码、分发唯一的识别符） * 将资产输入**资产管理**系统 * 将资产移到禁入区（如**仓库**、保险箱） | * 将接收到的不能立即贴上标签，并不能立即储存到仓库的资产存放到安全的**暂存区**（如高安保的货笼） |
| PS-18.3 | 执行接收连夜货运的安全方法。 | * 确保只有需要的人员才能看到安排物品的预期接收时间表 |
| PS-19.0 | 标记 | 除非收到客户的指示，否则禁止在外包装上使用名字信息，包括化名（“别名”）。 |  |
| PS-20.0 | 包装 | 在封闭/密封的容器内运输所有客户资产，根据资产的价值使用上锁的容器，或客户指示的容器。 |  |
| PS-20.1 | 至少执行以下控制措施之一：   * 防拆封的胶带 * 防拆封的包装 * 防解封的封条（如以全息图的形式） * 安全容器（如带有密码锁的安全箱） | * 制定和传达计划，规定如何处理已被篡改的货物 * 向事件应对小组报告所有篡改事件 (MS-5.0) |
| PS-20.2 | 包装 | 使用热塑收缩包装来打包所有的货物，并且在最后运输前，检查包装，确保货物被充分地包裹。 | * 如果使用整装运输，利用热塑收缩包装来打包个人资产（例如，滑板、货盘）或每个转轴 |
| PS-21.0 | 运输工具 | 始终对汽车和卡车上锁，勿将包裹放置在汽车和卡车内看得见的部位。 | * 不得在无人照看的情况下离开包裹 |
| PS-21.1 | 运输工具须包括以下安全特性（例如，拖车）：   * 单独的驾驶室 * 载货区的门能够上锁和密封 * 对于高度安保货物的运输须使用 GPS | * 使用配有 GPS 追踪系统的车辆来运输内容敏感的资产和高价值的资产 |
| PS-21.2 | 对于存放高度敏感货物的货舱门要实行编号密封。 | * 要求保安记录并监督密封 * 对于高度敏感的包装，考虑利用其他的安全措施（例如，上锁/有防护的载货区、上锁的安全防护箱） |
| PS-21.3 | 在运送高度敏感内容到高风险地区时，要求安排安全护卫人员。 | * 雇佣的保安须足以能胜任保护高度敏感内容免受劫持、抢劫和导致内容遭窃的其他情况 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| DS-1.0 | 防火墙/广域网/  外围安全 | 采用带有访问控制列表及具有跟踪上传下载通信量能力的防火墙，将内部网络与外部网络/广域网隔离，以免未经授权访问任何内部网络。 | * 配置带有访问控制列表的**广域网防火墙，**除了本属于**缓冲区 (DMZ)** 的明显主机外，拒绝一切进入内部网的行为 * 配置**广域网**，禁止其直接联入内部的存储内容/制作网络 * 包括详细的广域网文档，准确地说明和描述连接至和来自所有外部设备的连接数量 * 必须配置防火墙规则，以生成所有通信量和所有配置变更记录，应至少每月检查一次相关记录 * 防火墙应订购防病毒和入侵检测更新，并至少每周更新一次 * 建议在防火墙配置中纳入下列内容“ * 反干扰过滤器 * 阻止非路由 IP 地址 * 阻止外部端口的内部地址 * 阻止 UDP 和 ICMP 重复请求 * 阻止未使用的端口和服务 * 阻止未经授权的 DNS 区域数据传输 * 采用出口过滤器，仅可从内部地址向外发送通信量 |

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| DS-1.1 | 防火墙/广域网/  外围安全 | 开发一个程序，用来每 6 个月对防火墙的访问控制列表 **(ACL)** 进行复核，确认其设置合适，且符合业务部门的要求。 | * 从防火墙和/或路由器中输出 **ACL** * 复查**ACL**，确认对网络的访问为妥当 * 要求管理人员就复核以及任何防火墙规则变更签字 * 相应地更新**ACL** |
| DS-1.2 | 默认情况下拒绝所有协议，仅在广域网及防火墙上启用特定的允许安全协议。 | * 限制所有未加密的通信协议，如**远程登录协议**和**文件传输协议** * 将未加密协议替换为加密版本 |
| DS-1.3 | 将外部可访问的服务器（如网络服务器）放置在**缓冲区**。 | * 隔离**缓冲区**的服务器，让每台服务器（如网络服务器等）只提供一种服务 * 实行 **ACL**，限制从**缓冲区**网络进入内部网络 |
| DS-1.4 | 执行程序，给网络基础设施设备（例如，防火墙、路由器、交换机等）、SAN/NAS（存储区域网络和网络附加存储）及服务器打补丁。 | * 执行定期（如每月一次）程序，鉴定、评估和测试网络基础设施设备、SAN/NAS 及服务器的补丁 * 升级网络基础设施设备、SAN/NAS 及服务器的补丁水平，以解决重大的安全漏洞 * 在 48 小时内处理关键的补丁 * 建议部署集中管理的补丁管理系统 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| DS-1.5 | 防火墙/广域网/  外围安全 | 根据安全配置标准，加固网络基础设施设备、SAN/NAS 和服务器。如果未使用 SNMP（简单网络管理协议）或仅使用 SNMPv3 或更高版本，禁用 SNMP，并选择 SNMP 社区字符串，即更强的密码。 | * 考虑下列加固选项： * 禁用来宾账户及共享 * 安装防病毒/防恶意软件 * 启用软件防火墙 * 删除不需要的软件 * 卸载/禁用不需要的服务 * 要求所有用户作为受限用户运行软件 * 采用 **ACL** 限制对设备的访问，仅可使用授权管理系统连接使用 SNMP * 在加固网络基础设施设备时，参考以下的安全加固标准： * 美国国家标准技术研究院 * 存储区域网络 * 美国国家标准协会 |
| DS-1.6 | 不允许使用任何外部接口管理防火墙。 | * 而应使用二元认证并按 128 位或更多位的高级加密标准 (AES) 使用 **VPN** 连接，执行远程管理功能 * 要求非管理员远程访问的个人提供以下内容中的 2 个： * 个人所知信息（如用户名、密码） * 个人拥有的独特实体物件（如令牌、**钥匙卡**、智能手机、证明书） * 个人独有的体貌/生物学特征（如指纹、视网膜） |
| DS-1.7 | 防火墙/广域网/  外围安全 | 将网络基础设施 /SAN/NAS 设备和服务器安全备份到内部网络的中央安全服务器上。 | * 安装网络基础设施设备，将配置文件的备份以安全的方式（如加密）存储到内部网络 * 确保只有授权的管理员才能访问存储区域和加密备份 * 如果普通文件传输协议(TFTP)用来备份，确保限制条款到位，用以规避强力攻击和无授权访问配置文件的行为 |
| DS-1.8 | 至少每季度对所有外部 IP 范围和主机进行一次漏洞扫描，并纠正问题。 | * 及时纠正提供未经授权内容访问的关键问题 * 确保扫描/测试所使用的工具适应虚拟化技术（如使用） * 建议由独立的第三方执行此扫描/测试 |
| DS-1.9 | 至少每年对所有外部 IP 范围和主机进行一次渗透测试，并纠正问题。 | * 及时纠正提供未经授权内容访问的关键问题 * 确保扫描/测试所使用的工具适应虚拟化技术（如使用） * 建议由独立的第三方执行此扫描/测试 |
| DS-1.10 | 通过采用专用的私有连接和加密方式，确保任何点对点连接的安全。 | * 采用 128 位或更多位的高级加密标准 (AES) 进行加密 |
| DS-1.11 | 执行同步时间服务协议（例如网络时间协议），确保所有系统均有共同的时间参照物。 | * 确保系统拥有准确及一致的时间 * 确保时间数据得到保护 * 确保时间设置来自行业认可的时间来源 |
| DS-1.12 | 防火墙/广域网/  外围安全 | 制定、记录和实施适用于广域网网络基础设施设备和服务的基线安全要求。 | * 确保在投入制作前修改系统默认值可能出现的漏洞 * 建议持续监控，报告基础设施相对于安全基线的合规情况 |
| DS-2.0 | 互联网 | 禁止制作网络及管有或存储数字内容的所有系统直接访问互联网，包括电子邮件。如果某个业务案例需要制作网络或管有或存储数字内容的系统访问互联网，唯一批准的方法是通过远程托管应用程序/桌面会话访问。 | * 使用互联网网关系统（如 Citrix、Terminal Services、VNC 等）和以下控制措施 处理异常情况： * 系统受严格监控，服务器的唯一功能是浏览网页 * 禁止访问受限制的网站，包括网页式电子邮件网站、点对点网络、数字化储存网络，以及其他已知的恶意网站 * 限制内容被转入或转出系统 * 定期使用最新的病毒定义码修补和更新系统 * 定期检查系统的活动 * 阻止映射本地驱动器、阻止 USB 大容量存储器、阻止映射打印机、阻止复制粘贴功能、阻止通过制作网络下载/上传至互联网网关系统 * 实行**防火墙规则**，默认为拒绝所有输出通信量，明确允许要求向外传输的特定系统和端口连接至指定的内部网络（如防病毒定义服务器、补丁服务器、许可服务器（仅当无法使用本地许可时）等） |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| DS-2.1 | 互联网 | 使用电子邮件过滤软件或设备，阻止从**非制作网络**流出以下内容：   * 潜在的网络钓鱼电子邮件 * 禁止的文件附件（如 Visual Basic 脚本、可执行文件等） * 将文件大小限制在 10 MB * 以恶意软件或病毒来源著称的网域 | * 识别电子邮件附件和邮件信息主题中的受限制内容类型 * 实施电子邮件过滤解决方案，然后根据受限制的内容类型进行配置 |
| DS-2.2 | 安装网络过滤软件或设备，限制访问以点对点文件交易、病毒、黑客行为和其他恶意网站著称的网址。 | * 执行网络过滤软件/代理服务器软件，监测和预防访问恶意网站 |
| DS-3.0 | 局域网/内部网络 | 将**内容/制作网络**与**非制作网络**（例如，办公网络、**缓冲区网络**、互联网等）隔离 使用物理网络或逻辑网络进行分割。 | * 从需要访问的特定主机（如防病毒服务器、补丁管理服务器、内容发送服务器等）中定义出能够明确允许访问**内容/制作网络**的访问控制列表 * 纳入已明确定义的端口和服务，能够允许进入**访问控制列表** * 根据已定义的安全区域，分割或隔离网络 * 实行**防火墙规则**，默认为拒绝所有输出通信量，明确允许要求向外传输的特定系统和端口连接至指定的内部网络（如防病毒定义服务器、补丁服务器、内容传输服务器、许可服务器（仅当无法使用本地许可时）等） * 实行**防火墙规则**，默认为拒绝所有输入通信量，明确允许要求向内传输的特定系统和端口连接至指定的内容传输服务器。 * 有关在制作区域访问互联网的指南，请参阅 DS-2.0 * 使用**交换机**上的媒体存取控制地址分配**静态 IP 地址** * 禁用**内容/制作网络**的**动态主机配置协议 (DHCP)** * 禁止任何制作电脑系统一次性连接至一个以上的网络 * 禁止在非制作网络上使用或存储内容 |
| DS-3.1 | 只有授权人员才能进入内容/制作系统。 | * 建议使用物理以太网电缆锁，确保网络电缆不会连接至替代/未经授权的设备 |
| DS-3.2 | 局域网/内部网络 | 限定只有需要执行工作职责的规定人员才能远程访问**内容/制作网络**。 | * 禁止远程访问内容/制作网络 * 保留允许进入**内容/制作网络**的**公司员工名单** * 制定管理程序，检查**内容/制作网络**内的远程访问系统活动 * 将远程访问系统配置为使用个人帐户 * 只有带有访问控制列表的单一方法能使用远程访问 * 如需要应急远程访问，实施下列内容： * 采用二元认证，最好基于证明书 * 阻止文件传输协议，包括 FTP、SSH、IRC、IM * **VPN** 配置决不允许分割通道 * 利用启动板/堡垒 (Launchpad/bastion) 主机模式作为媒介，连接至制作网络 |
| DS-3.3 | 采用交换机/第 3 层设备管理网络通信量，禁用**内容/制作网络**上的所有未使用的**交换机**端口，防止未授权设备进行数据包监测。 | * 要求设备管理员采用严格认证，包括： * 使用加密协议 * 哈希值 (Salted hash) 加密 * 为执行命令设置独立密码 * 连接到设备控制台，更新配置文件，禁用**交换机**的未使用端口 * 启用交换机/第 3 层设备登陆 |
| DS-3.4 | 限制使用非交换设备，如在**内容/制作网络**上的集线器和中继器。 | * 将所有的集线器/中继器替换为**交换机**或第 3 层设备 |
| DS-3.5 | 局域网/内部网络 | 禁止在**内容/制作网络**的计算机系统上使用双宿主机网络（网络桥接）。 | * 在网络层（如**路由器**、**防火墙**、**交换机**等）执行网络桥接，而不在一个计算机系统中使用多个**网络接口卡 (NIC)** |
| DS-3.6 | 在**内容/制作网络**上，实施基于网络的入侵检测系统或入侵预防系统 **(IDS/IPS)**。 | * 配置入侵检测系统或入侵预防系统，对可疑的网络行为进行警报或预防 * 为**IDS/IPS**订购防病毒/防恶意软件 * 至少每周更新一次 **IDS/IPS** 上的攻击签名定义/政策和防病毒/防恶意软件 * 记录 **IDS/IPS** 的所有活动和配置变更 * 在所有工作站上实施主机型入侵检测系统软件 |
| DS-3.7 | 如果未使用 SNMP（简单网络管理协议）或仅使用 SNMPv3 或更高版本，禁用 SNMP，并选择 SNMP 社区字符串，即更强的密码。 | * 采用 **ACL** 限制对设备的访问，仅可使用授权管理系统连接使用 SNMP |
| DS-3.8 | 在**局域网/内部网络**上安装系统前加固系统。 | * 请参阅 DS-1.5 了解建议 |
| DS-3.9 | 至少每年执行一次内部网络漏洞扫描并纠正任何问题 | * 确保扫描所使用的工具适应虚拟化技术（如使用） * 包括下列内容： * 制作网络 * 非制作网络 * 已连接机器/设备 * 未连接机器/设备 |
| DS-3.10 | 局域网/内部网络 | 确保本地局域网络 SAN/NAS、设备、服务器和工作站安全备份到互联网的中央安全服务器上。 | * 安装本地局域网络设备，将配置文件的备份以安全的方式（即加密）存储到互联网上 * 确保只有授权的管理员才能访问存储区域和加密备份 |
| DS-4.0 | 无线网络/无线局域网 | 禁止使用无线网络和在**内容/制作网络**中使用无线设备。 | * 只允许无线访客网络访问互联网，而不能访问**内容/制作网络** * 移除或禁用无线网络访问内容/制作网络中处理或存储内容的工作站/笔记本电脑 |
| DS-4.1 | 无线网络/无线局域网 | 为**非制作**无线网络（例如行政网络和访客网络）配置以下安全控制措施：   * 禁用 WEP / WPA * 仅启用 **AES**128 **加密 (WPA2)** 或更高加密级别 * 将“访客”网络与公司的其他网络分开 * 变更默认管理员登陆凭据 * 变更默认网络名称 **(SSID)** | * 考虑如下安全控制措施： * 使用非公司特定 **SSID** 名称 * 启用 IEEE802.1X 或 IEEE802.11i（如果该选项可用） * 使用 RADIUS 进行身份验证（如果该选项可用） * 启用 **MAC 地址过滤** * 将制作工作站和设备的无线 MAC 地址列入黑名单 * 只在要求的范围内配置无线接入点/控制器进行广播 * 在无线接入中使用 802.1X 框架，包括以下各项： * 用于身份验证、授权和计费的远程拨号用户服务 (RADIUS) * 用于管理用户帐户的轻量级目录访问协议 (LDAP) 服务器（如 Active Directory） * 用于生成和管理客户端和服务器证书的公钥基础设施 * 如果必须使用预共享密钥，请采取以下控制措施： * 为 WPA2 配置 CCMP **(AES-128)** **加密**或更高加密级别 * 设置复杂的密码（请参阅 DS-8.1 了解密码复杂性的建议） * 至少每隔 90 天及当**公司关键人员**离职时更改密码 |
| DS-4.2 | 无线网络/无线局域网 | 实施程序来扫描恶意无线接入点和修复任何验证过的问题。 | * 实施程序来漫游和扫描机构，以了解是否有未受保护的无线接入点 * 如有可能，配置一套集中式的无线访问解决方案（即无线控制器），一旦检测到恶意无线访问，它便会警告管理员 |
| DS-5.0 | I/O 设备安全 | 指定特定系统用来输入/输出 (I/O) 内容。 | * 使用 **ACL** 以允许**内容/制作网络**与用于特定源/目标 **IP 地址**的 I/O 系统**之**间的信息流通 |
| DS-5.1 | 在所有处理或存储内容的系统上阻断输入/输出 (I/O)、大容量存储器、外部存储器及移动存储设备（即，**USB**、**FireWire**、Thunderbolt、SATA、**SCSI** 等） 以及光学媒体存储器（即，DVD、Blu-Ray、CD 等），但用于 I/O 内容的系统除外。 | * 考虑以下阻断 **I/O 设备**的方法： * 更改注册表设置以限制基于 MS Windows 之系统的 **I/O 设备**的写入访问权限 * 为基于 Mac 的系统移除大容量存储文件以控制工作站的写入访问权限 * 使用组策略为采用 Microsoft Active Directory 或 Apple Open Directory 的系统禁用 **I/O 设备** * 如果阻断输出设备不可行，使用 I/O 端口监控软件检测端口使用情况 |
| DS-6.0 | 系统安全 | 在所有工作站、服务器及连接至 SAN/NAS 系统的任何设备上安装防病毒和防恶意软件。 | * 安装有集中管理控制台的企业版防病毒解决方案 * 建议安装端点保护软件 |
| DS-6.1 | 每天或更频繁地更新所有防病毒和防恶意软件定义码。 | * 将集中式防病毒管理控制台配置为每天至少下载和推送定义码一次 |
| DS-6.2 | 将文件存入**内容/制作网络**之前，扫描文件的内容，检查是否有病毒和恶意软件。 | * 对未与**内容/制作网络**连接的系统进行扫描 |
| DS-6.3 | 系统安全 | 执行下列扫描：   * 定期对所有工作站进行全系统病毒和恶意软件扫描 * 对连接至 SAN/NAS 的服务器和系统进行全系统病毒和恶意软件扫描 | * 配置防病毒和防恶意软件，在防病毒和防恶意软件策略的基础上进行全系统扫描 * 配置防病毒和防恶意软件，在闲置时期进行病毒查杀 |
| DS-6.4 | 实施程序来使用修复系统漏洞的安全漏洞补丁/最新资料定期更新系统（例如，文件传输系统、操作系统、数据库、应用程序、网络设备）。 | * 如有可能，使用集中式补丁管理工具（如 WSUS、Shavlik、Altiris）自动为所有系统部署补丁 * 从供应商和其他第三方处寻求补丁 * 部署前先对补丁进行测试 * 如有不修补系统的合法商业案例，则采取异常处理和补偿控制的措施 |
| DS-6.5 | 禁止用户成为其工作站上的管理员，除非软件需要（例如，ProTools、Clipster 和 Blu-Print、Scenarist 和 Toshiba 等授权软件）。软件提供商提供的文件必须明确声明需要管理权限。 | * 确保登录工作站的用户帐户没有跟系统管理员一样的特权 |
| DS-6.6 | 无人看管时，用电缆锁锁住处理内容的便携式计算机设备（如笔记本电脑、平板电脑、机箱）。 | * 将电缆锁牢牢锁在固定物上（如桌子） |
| DS-6.7 | 系统安全 | 对包含内容或与客户项目有关的敏感信息的笔记本电脑和便携式计算存储设备实施额外的安全控制措施。对所有笔记本电脑加密。使用硬件加密的便携式计算设备。在所有处理内容的笔记本电脑/移动设备上安装远程终止软件，以允许远程删除硬盘和其他存储设备的内容 | * 如果必须在不安全的场所使用笔记本电脑，对笔记本电脑设置密保屏幕 * 不得将笔记本电脑连接至任何公共无限网络 * 不使用时关闭笔记本电脑的电源，不得使用睡眠或休眠模式 |
| DS-6.8 | 限制 IT 管理人员的软件安装特权。 | * 严禁安装和使用未经批准的软件，包括流氓软件（如非法或恶意软件） * 至少每季度扫描一次所有存储已安装应用程序的系统 |
| DS-6.9 | 实施安全基线和标准来配置在内部设置的系统（如笔记本电脑、工作站、服务器、SAN/NAS） | * 开发用来反映所有系统的安全标准版本 |
| DS-6.10 | 应当卸载内容传输服务器上不必要的服务和应用程序 | * 检查所有内容传输服务器上安装的服务列表（即服务 MSc），卸载或禁用任何不需要的服务 * 检查所有内容传输服务器上安装的应用程序列表，卸载或禁用任何不需要的应用程序 * 检查启用的应用程序列表，以确保所有不必要的应用程序没有运行 |
| DS-6.11 | 维持系统资料库和系统组件 | * 至少每月更新一次资料库 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| DS-6.12 | 系统安全 | 每年或对基础设施做出重大变更时记录网络拓扑结构并更新图表。 | * 包括 WAN、DMZ、LAN、WLAN（无限网络）、VLAN、防火墙及服务器/网络拓扑结构 |
| DS-7.0 | 帐户管理 | 为管理员、用户及所有处理内容的**信息系统**和应用程序建立和实施帐户管理流程 | * 帐户管理的文档政策与程序针对以下几方面： * 新用户请求 * 用户访问权修改 * 用户帐户的禁用和启用 * 用户终止 * 帐户到期 * 休假 * 禁止多位用户共享任何用户帐户 * 将服务帐户限制为仅用于需要这些帐户的应用程序 * 至少启用以下基础设施系统和设备的日志记录功能： * 基础设施组件（如**防火墙**、身份验证务器、网络操作系统、包括 **VPN** 在内的远程访问机制） * 制作用操作系统 * 内容管理组件（如存储设备、内容服务器、内容存储工具、内容运送工具） * 接入互联网的系统 * 考虑使用一个服务器来管理一个中央资料库里的日志（如系统日志/日志管理服务器、安全信息和活动管理 (**SIEM**) 工具） |
| DS-7.1 | 帐户管理 | 保留帐户管理活动（如审核电子邮件、更改请求表）的可追踪记录。 | * 如有可能，保留所有帐户管理活动的管理审批和关联操作的记录 |
| DS-7.2 | 在理解使用需知后，按照最少特权原则分配唯一的凭据 | * 在理解使用需知后，至少为以下**信息系统**分配唯一的凭据： * 制作系统 * 内容管理工具 * 内容**传输工具** * 网络基础设施设备 * 登录和监控系统 * 客户端网络门户 * 帐户管理系统（如 Active Directory、Open Directory、LDAP） * 仅当绝对需要时才授予 **VPN** 远程许可 |
| DS-7.3 | 重新命名默认管理员帐户及其他默认帐户，仅在需要这些凭据的特定情况下使用这些帐户（如操作系统升级、补丁安装、软件升级）。 | * 参考所有的硬件和软件的文档以确定所有默认帐户 * 更改所有默认帐户的密码 * 如有可能，更改每一个帐户的用户名 * 闲置时禁用管理员帐户 |
| DS-7.4 | 划分职责以确保负责对访问信息系统进行分配的个人，其本身不是那些系统的终端用户（如员工不能分配访问自己）。 | * 如有可能，利用一支独立团队来授权访问信息系统 * 当职责划分难以做到时，实施其他的补偿性控制措施，如： * 监控公司员工和第三方员工的活动 * 保留并审查审计记录 * 实施实体分离 * 实施管理人员监督 |
| DS-7.5 | 帐户管理 | 监控和审计管理员和服务帐户活动。 | * 为支持记录的应用程序和系统启用监控控制 * 设置系统和应用程序以记录管理员的操作和档案，最少要记录以下信息： * 用户名 * 时间戳 * 操作 * 其他信息（操作参数） * 监控服务帐户以确保他们只用于预期目的（如数据库查询问题、应用程序到应用程序的通信） * 采用每月审查管理员和服务帐户活动的方法，以确定普通行为或可疑行为，以及调查可能的滥用行为 |
| DS-7.6 | 实施程序来审查所有处理内容的**信息系统**的用户访问权限，及移除任何不再需要访问权限的用户帐户，频率是每季度一次。 | * 删除由于工作调动或辞职的**公司人员**而不再需要访问的用户和/或**第三方员工**的**信息系统访问权限**。 * 删除或禁用超过 90 天没有使用的帐户 |
| DS-7.7 | 按每个项目审查内容的用户访问权限。 | * 删除由于项目完成而不再需要访问的用户的**信息系统访问权限** |
| DS-7.8 | 帐户管理 | 在技术可行的情况下，禁用或删除内容处理系统上的本地帐户 | * 使用集中式帐户管理服务器（即目录服务器，如 LDAP 或 Active Directory）来验证**信息系统**的用户访问权限 * 对于网络基础设备，在帐户管理上实施身份验证、授权与会计 (AAA) * 禁用来宾帐户 * 如果必须使用本地帐户（如可能），更改每个默认帐户的用户名和密码，禁用使用本地帐户通过网络登录系统的功能 |
| DS-8.0 | 身份验证 | 强制使用**唯一用户名**和密码访问**信息系统**。 | * 制定政策强制使用**唯一用户名**和密码访问所有**信息系统** * 将**信息系统**设置成需要身份验证，至少要使用**唯一的用户名**和密码 |
| DS-8.1 | 为获取**信息系统**访问权限实行严格的密码政策。 | * 制定由以下内容组成的密码政策： * 最小密码长度为 8 个字符 * 以下参数至少需包含 3 个：大写字母、小写字母、数字及特殊字符 * 密码最多可用 90 天 * 密码最少可用 1 天 * 最多 3 到 5 次无效登录尝试 * 如果用户账户因无效登录尝试而被锁定，应手动解除锁定，不得在一段时间后自动解除锁定 * 之前 10 个密码的密码使用记录 |
| DS-8.2 | 身份验证 | 对远程网络访问（如 **VPN**）实施双重身份验证（如用户名/密码和硬令牌） | * 要求远程访问的个人提供以下内容中的 2 个： * 个人所知信息（如用户名、密码） * 个人拥有的独特实体物件（如令牌、**钥匙卡**、智能手机、证明书） * 个人独有的体貌/生物学特征（如指纹、视网膜） * 使用二元认证并按 128 位或更多位的高级加密标准 (AES) 使用 **VPN** 连接，执行远程管理功能 |
| DS-8.3 | 对服务器和工作站使用有密码保护的屏幕保护程序或锁屏软件。 | * 通过人工或某种办法（如 Active Directory 组策略）将服务器和工作站设置为在闲置最多 10 分钟后激活保护密码的屏幕保护程序 |
| DS-8.4 | 考虑实施额外的身份验证机制，为广域网和局域网/互联网网络访问提供多层次的身份验证策略。 | * 考虑添加下列一个或多个： * 多因素身份验证 * 识别和访问管理系统 * 单点登录系统 * 识别联合标准 |
| DS-9.0 | 记录与监控 | 采用实时记录和报告系统来记录和报告安全事件；至少收集以下信息：   * 何时（时间戳） * 何地（来源） * 何人（用户名） * 何事（内容） | * 至少启用以下基础设施系统和设备的日志记录功能： * 基础设施组件（如**防火墙**、身份验证服务器、网络操作系统、远程访问机制（如 **VPN** 系统）） * 制作用操作系统 * 内容管理组件（如存储设备、内容服务器、内容存储工具、内容运送工具） * 接入互联网的系统 * 应用程序 |
| DS-9.1 | 使用一个服务器来管理一个中央资料库里的日志（如系统日志/日志管理服务器、安全信息和活动管理 (**SIEM**) 工具）。 |  |
| DS-9.2 | 将记录系统设置为：当发现安全事件时，自动发送通知，以帮助积极采取应对措施。 | * 定义要求调查的事件，对相应的人员启用自动通知机制；考虑以下情况： * 成功或不成功地尝试连接**内容/制作网络** * 异常的文件大小和/或当日内容运送时间 * 重复尝试访问未获授权的文件 * 尝试特权升级 * 使用一个服务器来汇总一个中央资料库中的日志（如系统日志/日志管理服务器、安全信息和事件管理 (**SIEM**) 工具） |
| DS-9.3 | 就记录和报告系统汇报的任何异常活动进行调查。 | * 把**事件响应**程序与处理发现的安全事件相结合 |
| DS-9.4 | 记录与监控 | 在所有的系统上实施记录机制用于：   * 密钥生成 * **密钥管理** * 供应商证书管理 | * 确保所有生成的密钥和添加的证书均可追踪到单个用户 |
| DS-9.4 | 每周检查所有记录，每天检查所有关键和重要记录。 | * 调查任何可能暗示有严重安全事故的异常活动 * 辨别任何目前还未预警的其他异常事件，并且设置记录和报告系统以发送有关这些事件的警报 * 将不同系统的日志联系起来以确定异常活动的模式 * 基于记录检查结果，适当更新 **SIEM** 设置 |
| DS-9.5 | 启用内部和外部内容传送和转移记录功能，至少要包含以下信息：   * 用户名 * 时间戳 * 文件名 * 源 **IP 地址** * 目标 **IP 地址** * 事件（如下载、查看） |  |
| DS-9.6 | 记录与监控 | 记录至少保留一年。 | * 寻求法律顾问的指导，以确定任何日志保留的法规要求 * 将内容日志存储在中央服务器中，而该服务器只有特定用户才能访问，且存放在控制进入的房间中 |
| DS-9.7 | 只有合适人员才能访问日志。 | * 维护访问控制列表，以确保只有有责任监控和检查日志的人员有权查看日志 * 职责划分以确保个人不负责监控自己的活动 * 通过对日志文件使用适当的**访问权限**来保护日志，以使其免受未授权删除或修改 |
| DS-10.0 | 移动安全 | 为访问或存储内容的移动设备制定一个 BYOD（携带自己的设备办公）政策。 | * 考虑实施移动设备防病毒/防恶意软件保护，包括： * 更新定义，包括 * 每天进行扫描 |
| DS-10.1 | 为访问或存储内容的移动设备编制一个获批准的应用程序、应用程序商店和应用程序插件/扩展列表。 | * 禁止安装未获批准的应用程序，亦禁止安装并非通过事前批准的应用程序商店获得的批准应用程序 * 考虑一个移动设备管理系统 |
| DS-10.2 | 维持访问或存储内容的所有移动设备的库存。 | * 包括操作系统、修补级别、已安装的应用程序 |
| DS-10.3 | 要求为整个设备加密，或者为将处理或存储内容的设备区域加密。 | * 考虑一个移动设备管理系统 |
| DS-10.4 | 防止绕过安全控制措施。 | * 防止使用越狱、根文件等 |
| DS-10.5 | 移动安全 | 如果移动设备遗失/被盗/受危害或在其他方面属必要，实施一个系统以执行远程擦除。 | * 提醒员工，如果对设备进行远程擦除，则非公司数据可能遗失 |
| DS-10.6 | 如果设备有十分钟未使用，将自动锁定。 |  |
| DS-10.7 | 管理所有移动设备操作系统补丁和应用程序更新。 | * 在设备制造商、运营商或开发商进行一般发布后，应用最新的可用安全相关补丁/更新 |
| DS-10.8 | 强制执行密码政策。 | * 参阅 DS-8.1 |
| DS-10.9 | 实施一个系统以执行移动设备的备存和存储。 | * 对备份加密，并将他们存储在安全的地方 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| DS-11.0 | 安全技术 | 确保收到指示后，安全技术（如破坏、可见/不可见**水印**）可用也获用。 |  |
| DS-11.1 | 使用至少一个 **AES** 128 位或更多位的**加密技术**来加密硬盘上的内容或者加密整个硬盘，通过以下任何一种方法：   * 基于文件的**加密**：（即给内容本身加密） * 基于驱动器的**加密**：（即给硬盘驱动器加密） | * 就外部硬盘而言，考虑购买预先加密的驱动器（如 Rocstor Rocsafe、LaCie Rugged Safe） * 加密硬盘上的所有内容，包括： * SAN / NAS * 服务器 * 工作站 * 桌面 * 便携电脑 * 移动设备 * 外部存储驱动器 * 采用一个或多个以下方法： * 基于文件的**加密**，如加密的 DMG 或加密的 ZIP 文件 * 使用软件进行基于驱动器的**加密** |
| DS-11.2 | 使用带外通信协议（例如，不与内容放在同一存储**媒介**上）发送解密密钥或密码。 | * 使用与内容传输所用方法不同的方法来发送解密密钥或密码 * 进行检查，以确保主要名字和密码都与项目和内容无关 |
| DS-11.3 | 安全技术 | 实施和记录关键管理政策和程序：   * 使用保护敏感内容或数据的加密协议，不论其位置在何处（例如，服务器、数据库、工作站、便携电脑、移动设备、传送数据、电子邮件） * 受信任设备的批准与撤销 * 内容密钥的生成、更新与撤销 * 内容密钥的内部与外部分发 * 将加密密钥与可识别的所有者绑定 * 划分职责，以区分主要管理与主要使用 * 主要存储程序 * 主要备份程序 | * 考虑为每个客户和关键资产设定唯一的加密密钥 * 防止未经授权地替代加密密钥 * 要求加密主要保管人正式承认他们理解并接受他们的主要保管人责任 |
| DS-11.4 | 使用至少一个 **AES** 128 位或更多位的**加密技术**来加密静止和移动的内容，包括虚拟服务器中的内容。 | * [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 | 安全技术 | 始终以下列一种或多种方式存储用于加密数据/内容的密钥和私钥（非公钥）：   * 使用与数据加密密钥一样安全性高的主要加密密钥来加密，该密钥须与数据加密密钥分开存储 * 在一个安全的加密设备内（例如主机安全模块 (HSM) 或 Pin 交易安全 (PTS) 互动点设备） * 根据安全行业公认的方法，拥有至少两个完整长度的主要部件或主要份额 |  |
| DS-11.6 | 确认在**受信设备列表 (TDL)** 当中的设备为妥当的设备且经由权利人的批准。 | * 要求客户提供一份受信任的内容回放设备的列表单 * 仅为在 **TDL** 当中的设备创建密钥传送消息 (KDM) |
| DS-11.7 | 确认内容密钥的有效性并且保证其到期日期与客户说明相一致 | * 要求客户提供内容密钥的到期日期 * 明确说明密钥最后的到期时间，以限制内容可供观看的时间 |
| DS-12.0 | 内容跟踪 | 实施一个数字内容管理系统，以提供数字内容的跟踪详情。 | * 记录签入/签出的所有数字内容 * 记录所有内容的数字位置 * 记录每次签出的预计持续时间 * 记录每笔交易的日期和时间 |
| DS-12.1 | 内容跟踪 | 将有关数字内容移动事务记录保留一年。 | * 包括下列内容： * 签入/签出的日期和时间 * 签出资产人员的姓名和唯一身分证明 * 签出原因 * 内容位置 |
| DS-12.2 | 定期检查数字内容资产管理系统的记录并且调查异常情况。 |  |
| DS-12.3 | 适用时在数字资产跟踪系统中使用客户 AKA（“化名”）。 | * 只让参与处理客户资产的员工知晓客户的 AKA |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| DS-13.0 | 传输系统 | 只能使用获得客户批准的**传输**系统，系统设定有访问控制、使用至少一个 **AES** 128 位或更多位的加密技术来加密静止和移动的内容，内容传输会话使用安全性高的身份验证。 | * 只允许获得授权的用户访问内容传输系统 * 亦在项目基础上考虑限制访问 * 在使用前，向客户核实内容传输系统是否已获批准 |
| DS-13.1 | 必须要在获得客户预先书面审批的情况下，才能实施异常处理办法以应对未使用加密**传输工具**的情况。 | * 使用随机产生的用户名和密码（已获安全传输）来进行身份验证 * 只使用客户批准的传输工具/应用程序 * 对于必须使用未加密**传输工具**的例外情况，要求客户签字 * 文档和档案全部除外 |
| DS-14.0 | 传输设备的使用方法 | 实施和使用内容传输专用系统 | * 确保编辑站和内容存储服务器不用来直接传输内容 * 禁用 **VPN**/远程访问传输系统或用于存储、传输或操作内容的任何系统 |
| DS-14.1 | 将内容传输系统与行政和制作网络分开。 | * 从物理上或逻辑上分隔网络 |
| DS-14.2 | 传输设备的使用方法 | 将内容传输系统放置在**缓冲区 (DMZ)**，而不是**内容/制作网络**。 | * 放到 **DMZ** 之前先强化内容传输系统（参阅 DS-1.5，寻求建议） * 实施**访问控制列表 (ACL)**，限制除内容**传输工具**所需的端口以外的所有端口 * 使用**ACL** 将内部网络与 **DMZ** 之间的通信限定于特定源/目标 **IP 地址** * 禁止从用于传输内容的系统访问互联网，下载客户内容或访问经批准的内容传输位置所需的访问除外 |
| DS-14.3 | 成功传输/接收后，立即删除内容传输设备/系统上的内容 | * 要求客户收到内容后给予回复 * 实施从传输设备和系统上删除（包括从回收站删除）内容的程序 * 在合适的情况下，项目完成后立即解除客户访问**传输工具**的权利 * 确保会话结束后连接断开 |
| DS-14.4 | 自动向制作协调员发送有关信息输出的消息。 | * 将内容传送系统设置为，每次一位用户向外部发送内网的内容时都自动发送通知（如电子邮件）给制作协调员。 |
| DS-15.0 | 客户门户 | 对用以将内容、流媒体内容和分配的密钥传输给授权用户的网络门户进行访问限制。 | * 在网络门户周围实施访问控制措施，通过以下一种或多种措施传输内容、流式传输内容和分配密钥： * 需要用户凭据 * 整合用来身份验证和授权的设备和/或用户密钥 * 通过适当划分职责（例如，一个人应设立密钥，另一个人应使用密钥来加密内容）来管理加密密钥 * 限制访问特定的网络、**VLAN**、子网和/或 **IP 地址**的范围 * 在合适情况下，限制从客户门户网站上传/下载的能力 |
| DS-15.1 | 客户门户 | 向门户网站用户分配唯一凭据（如用户名和密码），向客户端安全地分配凭据 | * 不要在内容链接中嵌入用户名和密码 * 考虑通过不同的电子邮件分开发送用户凭据和内容链接 * 考虑通过手机或 SMS 分配用户凭据 * 考虑通过带外传输分配加密密钥 * 制定由以下内容组成的密码政策： * 最小密码长度为 8 个字符 * 以下参数至少需包含 3 个：大写字母、小写字母、数字及特殊字符 * 密码最多可用 90 天 * 密码最少可用 1 天 * 最多 3 到 5 次无效登录尝试 * 如果用户账户因无效登录尝试而被锁定，应手动解除锁定，不得在一段时间后自动解除锁定 * 之前 10 个密码的密码使用记录 |
| DS-15.2 | 确保用户只拥有访问其自身**数字资产**的权利（如客户 A 绝无权利访问客户 B 的内容） | * 至少按季度实施程序来检查文件/目录权限 * 确保只允许确有要求的人访问 |
| DS-15.3 | 将网络门户放到 **DMZ** 里的专用服务器上，将访问限定于往来特定 **IP** 和协议的访问。 | * 使用**访问控制列表 (ACL)**，限制除客户门户网站所需端口之外的所有端口 * 使用**ACL** 将内部网络与 **DMZ** 之间的通信限定于特定源/目标 **IP 地址** * 放到 **DMZ** 之前先强化系统（参阅 DS-1.5，寻求建议） |
| DS-15.4 | 客户门户 | 除非客户事先批准，否则禁止使用位于互联网网络服务器上的第三方制作软件/系统/服务。 | * 考虑添加下列一个或多个： * 多因素身份验证 * 识别和访问管理系统 * 单点登录系统 * 识别联合标准 * 按 128 位或更多位的高级加密标准 (AES) 使用 **VPN** 连接 |
| DS-15.5 | 为内/外网络门户使用 **HTTPS** 和强制使用高难度密码组（如 TLS v1）。 |  |
| DS-15.6 | 不要使用永久性 cookie 或以纯文本存储凭据的 cookie。 | * 通过现存的基于网络的应用程序查看 cookie 的使用情况，确保它们没有以纯文本来储存凭据 * 如果应用程序将凭据存储在纯文本 cookie 中，那么请采取以下措施中一种： * 重新配置应用程序 * 更新应用程序 * 向应用程序开发商索要安全补丁 |
| DS-15.7 | 如能配置，将内部或外部门户的内容访问权设置成到预定时间间隔时自动失效 |  |
| DS-15.8 | 每季度检测网络应用程序的漏洞，修复所有经过验证的问题。 | * 使用行业认可的测试指南，如开放网络应用安全项目 (OWASP) 所发行，用以确定普通网络应用程序漏洞（如跨站脚本 (XSS)、SQL 攻击和跨站请求伪造 (CSRF)）的指南 * 测试应由独立第三方执行 * 有关更多信息，请参阅附录 G |
| DS-15.9 | 客户门户 | 每年执行网络应用程序的渗透测试，修复所有经过验证的问题。 | * 使用行业认可的测试指南，如开放网络应用安全项目 (OWASP) 所发行，用以确定普通网络应用程序漏洞（如跨站脚本 (XSS)、SQL 攻击和跨站请求伪造 (CSRF)）的指南 * 测试应由独立第三方执行 * 有关更多信息，请参阅附录 G |
| DS-15.10 | 只允许授权人员请求与电信服务提供商建立连接。 |  |
| DS-15.11 | 禁止使用电子邮件（包括网络邮件）传输内容。 | * 考虑使用安全电子邮件应用服务器（如 Cisco IronPort、Sophos E-Mail Security Appliance、Symantic PGP Universal Gateway Email），加密电子邮件和附件 |
| DS-15.12 | 至少每季度检查一次对客户门户网站的访问情况 | * 一旦项目完成，解除访问客户门户网站的**访问权限** * 删除所有非活动帐户。 * 考虑每当传输数据时，向适当的一方自动传输电子邮件通知 |

附录 A — 术语表

本术语表中的基本术语和首字母缩略词经常在本文件中用到和提及。这些定义取自相关的 ISO 标准(27001/27002)、安全标准（如 NIST）和行业最佳实践。在最佳实践指南中，所有包含在此表中的术语用**粗体**突出显示。

| **术语或首字母缩略词** | **说明** |
| --- | --- |
| **访问控制列表 (ACL)** | 通过列出允许访问资源的系统实体身份，来对系统资源的访问实施控制的机制。 |
| **访问权限** | 对使用/修改某一对象或系统的许可。 |
| **高级加密标准 (AES)** | 使用 128 位数据块和 128 位、192 位或 256 位长度密钥之 NIST 对称密钥加密标准。 |
| **资产管理** | 从收购到处理完成，贯穿整个工作流程的资产跟踪系统。 |
| **闭路电视 (CCTV)** | 将信号传递到一组有限的显示器上特定位置的摄像机。 |
| **闭路电视控制台** | 中央闭路电视监控界面系统。 |
| **公司员工** | 任何直接效力于该机构的个人，包括员工、临时工和实习生。 |
| **内容/制作网络** | 用来存储、转移或处理媒体内容的计算机网络。 |
| **数字内容资产** | 任何形式的已经被格式化成二进制源代码（包括使用它的权利）的内容和/或媒体。 |
| **尽职调查** | 为确保良好信誉，在雇佣应聘员工或第三方员工前进行的研究或调查。 |
| **动态主机配置协议(DHCP)** | 自动给网络上的所有节点分配 IP 地址的协议。 |
| **缓冲区 (DMZ)** | 实体或逻辑子网，其包含一个公司针对一个更大的不受信任网络（通常指的是因特网）的外部服务。 |
| **加密** | 将数据转换成未授权的人员无法轻易理解的密码形式。 |
| **指纹识别** | 软件识别、提取，然后压缩一种媒体特性组分的技术，使得媒体只能通过其合成压缩形式才能被辨别出来。 |
| **防火墙** | 依据本地安全政策，限制网络之间访问的网关。 |
| **防火墙规则集** | 防火墙用来决定如何在数据源与目的地之间为数据包分配路线的指令表。 |
| **FireWire** | 允许外部设备向计算机传输数据的高速接口。 |
| **文件传输协议 (FTP)** | 规定文件在不加密的情况下在整个网络传输的 TCP/IP 协议。 |
| **HTTPS** | 通过计算机网络,尤其是对互联网的广泛部署进行安全通信的通信协议。 |
| **身份识别卡** | 用来识别经授权访问机构的个人（如员工、供应商、访客）。 |
| **入侵检测/入侵预防 (IDS/IPS)** | 入侵检测系统(IDS)是监控网络或系统活动是否存在恶意活动或政策违规行为,并向管理站发送监控结果报告的一种装置或软件应用程序。入侵预防系统(IPS)执行相同的功能，并且尝试阻止该活动。 |
| **事件响应** | 对安全事件的检测、分析和补救。 |
| **信息系统** | 机构用来处理信息的任何电子系统或基于计算机的系统。其中，信息系统包括应用程序、网络设备、服务器和工作站。 |
| **I/O 设备** | 用来与计算机交流的设备和/或计算机之间交流的设备（如 USB 和 FireWire 驱动器）。 |
| **IP 地址** | 分配给参与计算机网络的设备的数字识别（逻辑地址）。 |
| **密钥管理** | 制作、分配、存储和注销用来访问加密内容的密钥。 |
| **钥匙卡** | 与电子访问控制锁一起使用的存储数字签名的塑料卡。 |
| **局域网 (LAN)** | 覆盖一小片物理区域（如一间办公室）的计算机网络。 |
| **MAC 地址过滤** | 用来限制访问计算机网络的安全访问控制法。 |
| **主密钥** | 能够打开任何给定机构的所有门的密钥。能访问所有高级别安全区域的密钥也被认为是主密钥。 |
| **媒介** | 实体设备或书写表面，包括但不限于能记录、存储或打印一个系统内的信息的磁带、光碟、磁盘、LSI 存储芯片和打印输出。 |
| **网络协议** | 控制和启用计算端点之间的连接、通信和数据传输的协议或标准。 |
| **网络接口卡 (NIC)** | 将电脑与计算机网络相连接的一种电脑硬件组件。 |
| **非制作网络** | 所有没有被用来处理或传输媒体内容的计算机网络。非制作网络可以包括办公室网络或行政网络以及客户网络 |
| **风险评估** | 执行风险识别和轻重分级来确定对业务的可能威胁。 |
| **风险管理** | 通过风险评估和实施安全控制措施来识别、分析和降低风险。 |
| **路由器** | 硬件和软件被定制成承担引导信息和转发信息的任务的设备。 |
| **安全信息和事件管理 (SIEM)** | 该词指将安全信息管理(SIM)与安全事件管理(SEM)相结合的软件产品和服务。SIEM 技术提供对网络硬件和应用程序生成的安全警报的实时分析 |
| **职责划分** | 没有一个人应当具有独自完成一项任务的能力的原则；没有一个人应当对多个相关工作负责的原则。 |
| **服务集标识符 (SSID)** | 无线 LAN 的一个唯一标识符，通常是人工可读的字符串，因此通常被称为“网络名称”。 |
| **小型计算机系统接口 (SCSI)** | 计算机与外围设备之间的物理连接和传输数据标准。 |
| **暂存区域** | 内容在被取走（如，发送或收录）之前存放的区域。 |
| **静态 IP** | 使一台计算机每一次联网时使用相同 IP 地址的配置。 |
| **交换机** | 连接一个网络内的多台设备及将网络数据导向特定目的地的计算机网络设备。 |
| **远程登录协议** | 在互联网或局域网上使用的访问远程计算机的网络协议。 |
| **第三方员工** | 为外部公司工作的，被机构雇用提供服务的任何人员。第三方员工包括承包商、自由职业者和临时机构。 |
| **跟踪机制** | 在整个生产过程中跟踪资产的工具、程序和/或方法，包括资产登记、资产转移的跟踪（如将资产从仓库移到编辑站）、运送和资产销毁。 |
| **传输工具** | 通过网络，以电子方式传输数字内容资产的工具，通常伴有可验收的加密和身份验证机制。 |
| **传输协议** | 在计算机网络或互联网上传输文件时所涉及的程序 |
| **受信任设备列表 (TDL)** | 获批准用以回放内容的具体数字设备列表。 |
| **唯一用户名** | 可辨识的登录身份识别。 |
| **通用串行总线 (USB)** | 将设备连接到主机上的串行总线标准。 |
| **用户访问管理** | 生成、更改访问权限，从系统或应用程序中删除用户帐户的程序。 |
| **仓库** | 专门用来存储载有内容的传统媒体的区域。 |
| **虚拟局域网 (VLAN)** | 有 LAN/内部网络的特性但不受限于物理位置的计算机网络。 |
| **虚拟专用网络 (VPN)** | 允许用户访问另一个较大网络的计算机网络 |
| **广域网 (WAN)** | 覆盖面广（如一家公司）的计算机网络。 |
| **水印** | 将信息嵌入到数字资产的（可能为）不可逆过程。 |
| **在制品 (WIP)** | 任何被认为不是成品的商品。 |
| **工作流程** | 一家公司对内容实施的一系列步骤。 |

附录 B — MPPA 影片和发行渠道定义

**影片类型**

| **影片类型** | **说明** |
| --- | --- |
| **故事片** | 剧院发行或直接向家庭视频或互联网发行的一类作品，包括以下类型：   |  |  | | --- | --- | | **故事片类型** | **说明** | | 故事片 | 一部未删节版电影。 | | 短片 | 比一般故事片要短的影片。 | | 非故事类长片 | 其他作品，如一部纪录片。 | |
| **电视剧集** | 与电视、网络或手机相关的一类作品，包括某个季度剧集或迷你系列剧集。一个试播节目也跟其他专业系列（如“网络视频短片”或“手机短剧”）一样的也是一部剧集。 |
| **非剧集电视节目** | 与电视、网络、或手机有关的一类作品，但没有剧集（如，电视电影、体育赛事或新闻节目）。 |
| **宣传/广告片** | 这类作品包括：   * + “宣传片”—任何与媒体有关的宣传资料。包括片头、预告片、电子宣传资料袋和其他材料。宣传片是‘广告片’的一个特例。 |
| **广告片** | 任何形式的广告，包括电视广告、信息广告、公共服务通告和不涵盖于“宣传片”中的促销广告。这不包括电影预告片和片头，即使他们可能会像商业广告一样播放。 |
| **音乐片** | 包括铃声、音乐视频和其他音乐在内的一类作品。 |
| **其他类型** | 这类作品包括：   |  |  | | --- | --- | | **类型** | **说明** | | 选录作品 | 主要由另一部或多部作品的一部分或多部分构成的资产。 | | 补充材料 | 旨在对另一作品进行补充的材料。比如，与 DVD 相关的额外材料。 | | 集合 | 不属于另一类别的资产集合。比如，电影集。 | | 特许作品 | 其他类型的集合或组合。例如，特许作品可能包括多个电视节目，或多个电视节目和电影的组合。 | |

**发行渠道**

| **发行渠道** | **说明** |
| --- | --- |
| **剧场型** | 仅在电影院发行的故事片。 |
| **非剧场型** | 以除了电视播放、家庭播放或剧场上映以外的任何方式公开发行的电影。包括电影在以下地方上进行展播：(i) 在飞机上、火车上、船上以及其他常见运输工具上，(ii) 在学校、大学及其他教育机构里，在图书馆、政府机构、商业和服务组织及俱乐部里，在教堂及其他宗教导向的组织里，在博物馆里，在电影界（包括通过此类展播起源地邻近区域内的闭路电视进行的展播），(iii) 在永久的或临时的军事设施、封闭机构、退休中心、离岸钻井平台、伐木场以及远程林业基地和施工基地（包括通过此类展播起源地邻近区域内的闭路电视进行的展播）。 |
| **家庭播放视频** | 批发层面，为零售和租赁销售包装商品而发行电影，如 DVD 或蓝光光碟。 |
| **免费电视** | 通常按照与网络、电视台或基本有线电视网络签订的许可协议，通过免费的广播电视向公众发行电影。 |
| **付费电视** | 以要求广播链中至少一名参与者支付费用的方式向公众发行电影，如视频点播、有线电视、卫星转播、付费节目服务。 |
| **互联网** | 以下列任何一种在线发行渠道发行一部电影：   |  |  | | --- | --- | | **类型** | **说明** | | 电子零售 (EST) 或通过下载拥有 (DTO) | 网上出售的永久数字拷贝版 | | 在线租赁或视频点播 (VOD) | 在线支付租金，临时观看 | | 订阅视频点播 (SVOD) | 在线订阅付费的在线观看。 | | 在线免费点播 (FVOD) | 通常由广告收入支撑的免费在线流媒体观看。 | | 其他类型 | 在线媒体和新媒体，如移动或互联网协议电视。 | |

附录 C — 机构指示图

机构须审查说明，而该说明用以指导如何确认哪种类型与机构提供的服务相对应，并且在风险评估的基础上，采取适当的控制措施。

|  |  |  |  |
| --- | --- | --- | --- |
| **说明** | | | |
| ADS | 音频、配音和字幕 | FL | 电影实验室 |
| CA | 创意广告 | IFE | 机上娱乐 (IFE) 及接待服务 |
| CDF | 配送、交付、货运 | PP | 后期制作 |
| D | 发行 | R | 复制 |
| DC | 数字影院 | VFX | 视觉特效 |
| DS | 数字内容服务 | AS | 应用程序安全 |
| DVD | 数字视频光盘制作 | CS | 云安全 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 |

附录 D — 控制措施的参考指示图

下表就 ISO 27001/27002 和 NIST 800-53 标准提供了最佳实践的总指示图。欲了解更多关于实施所提供的安全控制措施的信息，请参阅这些标准。

| **编号** | **安全主题** | **ISO 27002 -2013 参考** | **NIST 800-53 Rev. 4 参考** |
| --- | --- | --- | --- |
| **MS-1.0** | 行政安全意识/监管 | 6.1.1 | PM-1, PM-2 |
| **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** | 风险管理 | 6.1.1 | CA-1, RA-1 |
| **MS-2.1** | 5.1.2 | RA-2 |
| **MS-3.0** | 安保组织 | 6.1.3 | PM-2 |
| **MS-4.0** | 政策与程序 | 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** | 事件响应 | 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** | 业务连续性和灾难恢复 | 17.1.1 | CP |
| **MS-6.1** | 17.1.1 | CP |
| **MS-7.0** | 变更控制和配置管理 | 14.2.2 | CM |
| **MS-8.0** | 工作流程 | 11.1 |  |
| **MS-8.1** | 11.1 |  |
| **MS-9.0** | 职责划分 | 6.1.2 | AC-5 |
| **MS-10.0** | 背景调查 | 7.1.1 | PS-3 |
| **MS-11.0** | 保密协议 | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-11.1** | 8.1.4 | PS-4, PS-8 |
| **MS-12.0** | 第三方的使用与筛选 | 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** | 入口/出口 | 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** | 访客进入/离开 | 11.1 | PE-8 |
| **PS-2.1** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-2.2** | 11.1 | PE-3 |
| **PS-2.3** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-3.0** | 身份识别 | 11.1.2 | PE-3 |
| **PS-4.0** | 外围安全 | 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** | 警报器 | 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** | 授权 | 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** | 电子准入控制 | 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** | 密钥 | 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** | 摄像头 |  | 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** | 记录与监控 | 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** | 搜查 | 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** | 库存追踪 | 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** | 库存盘点 | 8.1.1 | AU-6, CM-8 |
| **PS-13.1** | 6.1.2 | AC-5 |
| **PS-14.0** | 空白媒介/生胶片库存跟踪 | 8.2.2 | MP-4 |
| **PS-14.1** | 8.1.1 | MP-4, PE-2, PE-3 |
| **PS-14.2** |  |  |
| **PS-15.0** | 客户资产 | 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** | 处理 | 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** | 装运 | 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** | 接收 | 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** | 标记 | 8.2.2 | MP-3 |
| **PS-20.0** | 包装 | 8.3.3 | MP-5 |
| **PS-20.1** | 8.3.3 |  |
| **PS-20.2** |  |  |
| **PS-21.0** | 运输工具 |  | MP-5 |
| **PS-21.1** |  |  |
| **PS-21.2** |  |  |
| **PS-21.3** |  |  |
| **DS-1.0** | 外部网络/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** | 互联网 | 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/内部网络 | 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** | 无线网络 | 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** | I/O 设备安全 | 10.7.1 | SC-7 |
| **DS-5.1** |  | AC-19, MP-2 |
| **DS-6.0** | 系统安全 | 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** | 帐户管理 | 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** | 身份验证 | 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** | 记录与监控 | 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** | 移动安全 | 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** | 安全技术 | 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** | 内容跟踪 |  |  |
| **DS-12.1** |  |  |  |
| **DS-12.2** |  |  |  |
| **DS-12.3** |  |  |  |
| **DS-13.0** | 传输系统 | 10.1, 13.2 | IA-5, SC-13 |
| **DS-13.1** | 10.1, 13.2 |  |
| **DS-14.0** | 传输设备的使用方法 | 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** | 客户门户 | 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 |  |

附录 e — 常见问题

1. **我的机构需要执行列出的所有最佳实践吗？**

对最佳实践的遵守完全出于自愿，在计划、执行和修改安全程序时，这些指南只作参考。

1. **如果我的机构要提供多种服务（例如，电影实验室和后期制作），我应该采用哪一组增补最佳实践呢？**

除非工作流程彼此分离，否则机构应采用更严格的一组增补最佳实践；如果工作流程确实彼此分离，您只应该把增补最佳实践应用到所服务的环境中。

1. **我的机构需要应用最佳实践“实施指南”一节列出的所有项目吗？**

不需要。这部分指南中包含的信息旨在帮助您确定以最佳的方式来构建特定的安全控制措施。如果由 MPAA 对您的机构进行内容安全评估，我们的评估只需在给定的时间内把您机构的实际操作与指南中相应的最佳实践部分作比较。（欲了解关于如何收到 MPAA 内容安全评估的更多信息，请您登录 contentsecurity@mpaa.org，联系我们。

1. **如果我现在的系统不允许执行最佳实践，应该怎么办？**

请联系相应的系统供应商，确定合适的解决方案，使系统能够遵循最佳实践。解决的方案可包括打补丁、更新版本或重装一个更安全的系统。如果技术限制最佳实践的执行，可采用其他的安全措施，但是，通常情况下，这些措施可能不会覆盖到相关风险。因系统限制导致安全指南无法执行的特殊情况，应正式记录，并从客户处获取批准。

1. **根据此指南应用最佳实践时，我们的机构还需遵循由个别 MPAA 成员设定的安全要求吗？**

最佳实践的执行是一般性指南，它不能取代个别 MPAA 成员的具体合同条款。对于供应商的选择都是由每个成员单独决定的。MPAA 鼓励您把最佳实践作为指南，在您与客户于未来进行安全方面的讨论时作参考。

附录 f — 建议的政策与程序

下面是为了保护电影内容，应发展和实施安全政策和规章的一些常见领域：

1. **物理安全政策与程序**

* 入口/出口安全
* 访客访问协议
* 身份识别与授权
* 应急预案
* 机构准入控制
* 机构监控

1. **库存及资产管理**

* 库存追踪
* 装运协议
* 运输过程中的现场库存

1. **信息技术安全**

* 互联网使用政策
* 身份验证和授权
* 密码政策
* 恶意代码防护/防病毒
* 注意：包括所有方面（可接受的使用等）

1. **人力资源政策和规程**

* 包含工作职责中的安全
* 人员筛选
* 保密、产权和知识产权保护协议
* 聘用条款与条件
* 职责划分 (SOD)
* 雇佣终止
* 惩处措施
* 安全意识与培训项目
* 雇员和临时雇员/自由职业者背景调查与筛选
* 雇员和临时雇员/自由职业者的不披露协议 (NDA)
* 记录保留

1. **第三方**

* 第三方合同
* 不披露协议 (NDA)

1. **事件响应**

* 事件确认与分析
* 事件升级与报告
* 事件响应流程与程序
* 事后剖析审查程序和经验教训

附录 g — 其他资源和参考

国际标准化组织 (ISO)，标准 27001。*信息技术 - 安全技术 - 信息安全管理系统 - 要求。*2005 年 10 月。<http://www.27000.org/iso-27001.htm>

国际标准化组织 (ISO)，标准 27002*。信息技术 - 安全技术 - 信息安全管理的业务守则。*2007 年 7 月。<http://www.27000.org/iso-27002.htm>

国际标准化组织 (ISO)，标准 27005。*信息技术 - 安全技术- 信息安全风险管理*。2008 年 6 月。<http://www.27000.org/iso-27005.htm>

国家标准与技术特殊出版物研究所 800-53。*适用于联邦信息系统的建议安全控制措施*，2005 年 2月。 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

国家标准与技术特殊出版物研究所 IR 7298。*重要信息安全术语词汇表，*2006 年 4 月。

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

系统管理，审计，网络与安全（SANS 研究所）。*安全和入侵检测中使用的术语词汇表*

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

开放的网络应用安全项目 (OWASP) - 测试指导

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

国家标准与技术特殊出版物研究所 800-88。*媒体清洁处理指南*，2006 年 9 月。http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

国家工业安全计划- 工作手册 (DoD 5220.22-M)，2006 月 2 月

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

网络安全中心 – 安全基准 http://benchmarks.cisecurity.org/

国家安全局-安全配置指南 https://www.nsa.gov/ia/mitigation\_guidance/security\_configuration\_guides/

国家标准与技术特殊出版物研究所 800-92。*计算机安全日志管理指南，*2006 月 9 月。<http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

国家标准与技术特殊出版物研究所 800-44。*公共网络服务器的安全指引，*2007 年 9 月。<http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>

国家标准与技术特殊出版物研究所 800-40。*创建补丁和漏洞管理程序，*2005 年 11 月。<http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

附录 h — 向 MPAA 举报盗版

**MPAA 的在线盗版举报**

您可通过以下网址直接向 MPAA 举报盗版：

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

**MPAA 和 MPA 24 小时盗版举报热线**

下面列出了 MPAA 在当地与内容保护办公室有合作之国家和地区的 24 小时举报热线：

|  |  |
| --- | --- |
| **北美和拉美地区** | |
| 加拿大 | (800) 363-9166 |
| 美国 | (800) 371-9884 |
| **欧洲、中东、非洲(EMEA)地区** | |
| 比利时 | +32 2 778 2711 |
| 意大利 | (800) 864 120 |
| 荷兰 | (909) 747 2837 |
| 乌克兰 | +38 0 445 013829 |
| 英国 | (800) 555 111 |
| **亚太地区(APAC)** | |
| 澳大利亚 | +61 29997 8011 |
| 香港 | +65 6253-1033 |
| 马来西亚 | +65 6253-1033 |
| 新西兰 | +65 6253-1033 |
| 菲律宾 | +65 6253-1033 |
| 新加坡 | +65 6253-1033 |
| 台湾 | +65 6253-1033 |

所有内容保护的地区和国家办公室的完整联系信息列表位于：<http://www.mpaa.org/contact-us/>

**MPAA 在线资源**

关于 MPAA 的其他信息，也可在此网站查询：[www.mpaa.org](http://www.mpaa.org)

您可在访问下列网站时了解保护电影内容的全球项目：[www.fightfilmtheft.org](http://www.fightfilmtheft.org)

**完**