****

**MPAA 内容安全计划**

**维护内容安全的最佳实践**

 **应用程序和云端/分布式环境安全指南**

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

版本 1.0

2015 年 3 月 17 日

|  |
| --- |
| 文档历史记录 |

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **说明** | **作者** |
| 1.0 | 2015 年 3 月 17 日 | 首次公开发布 | 美国电影协会美国电影协会成员公司 |

|  |
| --- |
| **目录** |

[文档历史记录 ii](#_Toc430869244)

[I. 最佳实践概述 2](#_Toc430869245)

[II. 提供商概述 3](#_Toc430869246)

[III. 风险管理 4](#_Toc430869247)

[IV. 文档结构 5](#_Toc430869248)

[V. 最佳实践的格式 6](#_Toc430869249)

[VI. 最佳实践应用程序安全指南 7](#_Toc430869250)

[VII. 最佳实践云安全指南 23](#_Toc430869251)

[附录 A — 术语表 31](#_Toc430869252)

[附录 B — MPPA 影片发行渠道定义 38](#_Toc430869253)

[附录 C — 常见问题 40](#_Toc430869254)

[附录 D — 向 MPAA 举报盗版 41](#_Toc430869255)

|  |
| --- |
| 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）进行了网站安全测评。其成员公司包括：迪士尼电影、派拉蒙影业公司、索尼影视娱乐公司、二十世纪福克斯电影公司、环球影城有限责任公司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。其可通过以下方式实现：

* 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具体讨论。

**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。最佳实践分为**应用程序**及**云端/分布式环境**安全指南。**供应商必须首先接受最佳实践通用指南的评估。在两份指南均适用的情况下，以更严格的指南为准。**

**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

|  |
| --- |
| 提供商概述 |

下表就提供的典型服务、功能类型，以及与每种提供商类型有关的发布窗口做了说明。

| **编号** | **提供商类型** | **典型提供商服务** | **功能类型** | **服务交付时段** |
| --- | --- | --- | --- | --- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **应用程序** | * 应用程序开发
* 网络应用程序
* 企业资源规划 (ERP)
* 信息工作者软件
* SaaS（软件即服务）
 | * 应用程序开发环境
* 多样
* 多样
* 多样
* 多样
 | * 多样
* 多样
* 多样
* 多样
* 多样
 |
| **2** | **云端** | * IaaS（基础设施即服务）
* PaaS（平台即服务）
* SaaS（软件即服务）
* 私有云
* 公共云
* 混合云
 | * 数据存储、计算资源
* 应用程序开发环境
* 业务应用程序
* 多样
* 多样
* 多样
 | * 多样
* 多样
* 多样
* 多样
* 多样
* 多样
 |

**控制措施的适用性**

本文件中的指南（应用程序安全和云安全指南）适用于所有应用程序和云供应商。

|  |
| --- |
| 风险管理 |

**风险评估**

通过**风险评估**来预测风险，并执行适当的控制措施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 标准亦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**

在您们的机构，进行资产分类的过程有四步，总结如下：

资产识别和分类

监控和评估有效性

确定最低限度的安全控制集

实施控制

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
 |

**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通常取决于资产的分类、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控制措施。此外，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。本文件中概述的最佳实践基于开放的网络应用程序安全项目 (**OWASP**)、云安全联盟 (**CSA**)、**PCI 数据安全标准**、**NIST 800-53**、**SANS 关键安全控制措施**以及 **ISO 27002** 的指南。

|  |
| --- |
| 最佳实践应用程序安全指南**IV. 文档结构****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。在这个文件的背景下，该模型包括横跨两个领域的安全主题：应用安全和云安全。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, （即开放的网络应用安全项目（OWASP）, 云安全联盟是 (CSA), PCI 数据安全标准, NIST 800-54, SANS 关键安全控制措施）和行业最佳实践.** |



**第30页**

**第29-30页**

**第29页**

**第27-28页**

**第27页**

**第24页**

**第25-26页**

**第25页**

**第23-24页**

**第22页**

**第22页**

**第21页**

**第20-21页**

**第19页**

**第18页**

**第17-18页**

**第16页**

**第15-16页**

**第7-8页**

**第9页**

**第10-11页**

**第11页**

**第12页**

**第13-14页**

**第14页**

**第14页**

**操作**

**操作**

**组织与管理**

**安全编码和漏洞管理**

**身份验证和访问**

**开发生命周期**

**云安全**

**应用程序安全**

|  |
| --- |
| 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：

|  |  |
| --- | --- |
| 应用程序安全 | 云安全 |
| 开发生命周期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。 | 身份验证和访问 | 安全编码和漏洞管理  | 组织与管理 | 操作 | 数据安全 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| AS-2.7 | 身份验证和访问 | 使用人工验证工具（例如 **CAPTCHA** 或 **reCAPTCHA** 及网络应用程序 | * 使用 **CAPTCHA** 或 **reCAPTCHA**，以防止机器人程序攻击
 |

**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。

**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。

**最佳实践**

每个安全主题都有最佳实践的概述。

**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。

|  |
| --- |
| 佳实践应用程序安全指南 |

| **编号** | **安全主题** | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| AS-1.0 | 开发生命周期 | 在整个**系统/软件开发生命周期** (**SDLC**) 确保安全。 | * 考虑使用行业标准方法：
	+ **瀑布图**
	+ **快速应用程序开发** (**RAD**)
	+ **敏捷**
* 请参阅 **ISO/IEC 12207**，了解建立软件生命周期的流程及为软件系统的开发、购买和配置提供模型之实施指南
* 实施**职责划分**：
	+ 在规定/设计、建筑、测试、发布和维护阶段记录所有流程和数据（包括下列各项）：
* 程序更改请求
* 用户接受测试和批准
* 管理层批准
	+ 在生产环境中将开发环境与测试环境分隔开来。利用访问控制强制执行分隔。
	+ 确保生产数据不被用于开发和测试环境中。
* 在设计开始前，为系统/软件执行一项风险分析，包括以下各项：
	+ 威胁模型包括意料之中的漏洞和威胁
	+ 经过**应用程序**安全专业人员审核
	+ 安全和隐私要求
	+ 测试范围
* 使用安全编码标准
 |
| AS-1.0（续） | 开发生命周期 |  | * 实施**更改控制：**
	+ 记录所有迁移至生产的更改
	+ 限制访问进入生产的迁移更改
	+ 当做出更改时，重复进行测试，或者至少每季度测试一次
	+ 根据更改的影响准备撤回程序
* 执行测试：
	+ 在整个 **SDLC** 测试安全性，解决漏洞、威胁和隐私问题
	+ 执行手动及自动测试
	+ 执行自动安全测试，包括静态代码分析和动态代码分析
	+ 实施控制措施，为任何外包软件开发活动检测源代码安全缺陷
	+ 更正任何问题
* 防止**应用程序**代码详情被不当使用或披露：
	+ 为每位特权用户分配个别管理员帐户，以确保责任制
	+ 每季度审核所有用户的访问情况
	+ 在**应用程序**生效或向客户发布之前，删除开发、测试和/或自定义**应用程序**帐户、用户 ID 和密码
	+ 防止未经授权地访问**应用程序**/程序/源代码。仅向获授权人员提供代码
	+ 防止未经授权地访问租户**应用程序**、程序或目标源代码，以及确保仅向获授权人员提供
 |
| AS-1.1 | 开发生命周期 | 测试整个应用程序和基础设施内的安全性。 | * 确保范围包括以下各项：
	+ 应用程序服务器
	+ 数据库服务器
	+ 服务器操作系统
	+ 虚拟服务器组件
	+ 网络服务器（前端和后端）
	+ 企业架构组件（例如以服务为主导的架构）
* 当做出更改时，重复进行测试，或者至少每季度测试一次
 |
| AS-1.2 | 通过向系统大量输入随机数据，尝试使系统崩溃（例如**缓冲区溢出**、**跨站脚本**、**拒绝服务攻击**、**格式错误**、**SQL 攻击**），进行**模糊测试**和**缺陷修复**，以发现软件、操作系统或网络中的安全漏洞。 | * 提供意料之外输入的测试
* 评估应用程序如何反应
* 当做出更改时，重复进行测试，或者至少每季度测试一次
 |
| AS-1.3 | 进行**错误跟踪**和**缺陷修复**以及广泛的**黑盒测试**、**beta 测试**和其他行之有效的调试方法。 | * 获得关于功能性错误和安全漏洞的错误报告
* 修复缺陷
 |
| AS-1.4 | 就应用程序的增加和更改提供培训和用户指导。 |  |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| AS-2.0 | 身份验证和访问 | 实施安全**验证。** | * 用户名称/用户 ID：
	+ 禁止复制用户名称/用户 ID 的使用
	+ 禁止分享用户名称/用户 ID 以及同时使用同一用户名称/用户 ID
	+ 用户名称/用户 ID（不区分大小写）
* 按照以下规则使用密码控制措施：
	+ 密码长度最少有 8 个字符
	+ 考虑使用最长的密码长度
	+ 必须使用安全度高的密码，至少符合下列 5 项规则中的 3 项：
* 至少 1 个大写字符 (A-Z)
* 至少 1 个小写字符 (a-z)
* 至少 1 个数字 (0-9)
* 至少 1 个特殊字符（标点符号或一个空格）
* 一行中不超过 2 个相同字符
* 保留由至少 10 个密码组成的密码历史，不再使用这些密码
* 最长 90 天的失效期
* 在 5-10 次密码尝试失败后，锁定用户帐户。保持帐户的锁定状态，直至管理员手动解锁为止。
* 在处于不活动状态达 30 分钟后，自动注销用户。在登录 4 小时后，考虑注销用户或强制用户开始新会话（不论是否处于使用或不使用状态）。
* 安全地保存密码（例如，不采用纯文本形式，仅通过 **TLS** 传输密码）
* 就敏感功能要求重新**验证**
* 考虑使用 **SSL** 客户**验证**
 |
| AS-2.0（续） | 身份验证和访问 |  | * 使用目录服务，以进行**验证**
* 使用**多重身份**或**双重身份验证**：
	+ 须知事项（帐户详情或密码）
	+ 拥有的事物（令牌或智能手机）
	+ 您的身份（生物特征）
* 考虑实施身份和访问管理 (**IAM**) 系统，自动地发起、捕获、记录及管理用户及其访问许可，以确保下列各项：
	+ 根据政策诠释授予特权
	+ 所有人士和服务均经过适当地验证、授权和审计
 |
| AS-2.1 | 登记用户设备。 | * 登记应用程序用户使用的设备，包括但不限于：
	+ 设备 ID 或硬件 ID
	+ **IMEI**（国际移动设备识别码）或 **MEID**（移动设备标识符）
	+ **MAC**（媒体访问限制）**地址**
* 在验证过程中，对照用户的已知设备清单检查正在使用的设备
* 使用多重身份**验证**（例如，带外提供的一次性密码、智能手机 PIN 码），允许用户安全地登记新设备
* 在切实可行的情况下，考虑将用户帐号固定到一个或两个用户设备
* 考虑限制每个用户的设备数量（例如每个用户最多五个设备）
* 防止用户在一个以上的设备上同时发起会话
 |
| AS-2.2 | 身份验证和访问 | 实施安全密码恢复。 | * 考虑下列步骤：
	+ 收集用户提出的问题、封闭式问题或识别数据问题（了解隐私顾虑）
	+ 问题的答案尽量简洁
	+ 验证安全问题和回答
	+ 设计问与答的存储系统
	+ 考虑让用户定期审核和更新问与答
	+ 验证更改问题的请求（可能使用端通道），例如向智能手机发送的 pin 码
	+ 立即锁定用户帐户，通过端通道发送一个令牌
	+ 允许用户在现有会话中更改密码
	+ 测试密码恢复程序，以防范**社会工程**
	+ 核实安全问题库不包括关于学校、出生日期、婚前姓的问题或者可通过 LinkedIn、Facebook 等互联网网站访问的任何其他记录。
 |
| AS-2.3 | 遵守最小特权原则。 | * 使用用户帐户（而非特权帐户）以及最低可能的许可水平来操作应用程序
* 禁止使用系统或管理员水平的许可来运行应用程序
 |
| AS-2.4 | 实施控制措施，以防止暴力攻击。 | * 在数次错误的密码尝试后锁定用户帐户；考虑将 5-10 次设为门槛值
* 考虑保持用户帐户的锁定状态，直至管理员手动解锁为止
 |
| AS-2.5 | 身份验证和访问   | 实施和记录流程，以实现安全的钥匙/密码存储，确保持续地安全管理。 | * 仅存储要求保存的敏感性数据
* 在存储数据时考虑隐私问题
* 支持租户生成的**加密**密钥，或者允许租户将某个身份的数据加密，而无需访问公钥证书（例如以身份为基础的**加密**）
* 仅使用安全度高的加密算法（例如，**AES**、RSA 公钥加密、SHA-256 或更好的算法）
* 不使用安全度低的算法（例如 MD5 或 SHA1）
* 确保随机生成的数字（用于文件名或 GUID）被高度加密
* 仅使用被公认的加密算法（参阅 NIST FIPS 140-2）
* 存储密码的哈希值和盐值，而非密码本身。
* 即使初步控制措施失败，也要确保加密存储保护的安全（例如，总是加密静态数据）
* 确保密钥未被未经授权地访问
* 界定一个关键的生命周期：
	+ 在其生命周期中记录关键的处理程序
	+ 记录处理关键泄露的程序
	+ 使用集中式、自动化**密钥**管理方法（与手动密钥分布相反）
	+ 保护**仓库**中的密钥
	+ 将密钥与它们用于加密的数据分开存储
	+ 不在应用程序服务器、网络服务器、数据库服务器等服务器上存储密钥
 |
| AS-2.5（续） | 身份验证和访问 |  | * + 建议就每个租户甚至每个项目创建唯一的**加密**密钥
	+ 定期更改密钥（至少每一至三年更改一次）
	+ 至少每一至三年更新一次数据
	+ 就创建、管理和使用密钥**划分职责**
	+ 要求主要保管人就其相关职责和责任签署一份表格
	+ 仅使用安全的方法来分配密钥（例如 **TLS**）
	+ 在要求提供多种密钥时使用独立的密钥（例如，不选择与第一个密钥有关的第二个密钥）
	+ 防止未经授权地替代密钥
 |
| AS-2.6 | 启用自动失效设置，在用户规定的时间后，连接至内容的所有外部链接将失效。 | * 链接失效的默认设置时间是 24 小时
 |
| AS-2.7 | 使用人工验证工具（例如 **CAPTCHA** 或 **reCAPTCHA**）及网络应用程序。 | * 使用 **CAPTCHA** 或 **reCAPTCHA**，以防止机器人程序攻击
 |
| AS-2.8 | 让客户能够限制某个用户下载或进行流式传输资产的次数。 |  |
| AS-2.9 | 身份验证和访问 | 确认上传和下载所有内容和关键资产。 | * 一旦内容被上传、下载或查看，立即向内容所有者、项目所有者或项目经理发送电子邮件
* 包括下列详情：
	+ 所有活动的准确时间戳
	+ 根据访问规则下载/流式传输尝试（成功和失败）
	+ 法证信息（例如，**IP** 或 **MAC 地址**、**地理位置**信息）
	+ 每个用户每项资产下载/流式传输尝试的次数
 |
| AS-2.10 | 包括关于移动应用程序的简要讯息，以提醒用户启用设备密码，以及启用远程擦除和设备位置软件。 | * 提醒用户安装位置和远程擦除工具，例如 **查找我的 iPhone**、**Android 设备管理器**
* 安装、配置和保持一个**移动设备管理**系统
 |

| 编号 | 安全主题 | 最佳实践 | 实施指南 |
| --- | --- | --- | --- |
| AS-3.0 | 安全编码和系统 | 在生产部署前执行**渗透测试**/**网络应用程序安全测试**，之后至少每个季度执行一次测试。使用重新测试，确认漏洞被修复。 | * 使用网络安全行业标准工具
* 就 **OWASP** 的十大安全隐患进行测试：
	+ A1 注入（包括 SQL、OS 和 LDAP）
	+ A2 XSS
	+ A3 安全度低的**验证**和**会话管理**
	+ A4 不安全的直接目标参考
	+ A5 跨站请求伪造
	+ A6 安全错误配置
	+ A7 不充分的加密存储
	+ A8 未能限制 **URL** 访问
	+ A9 不充分的传输层保护
	+ A10 未经验证的跳转
	+ 参见更新：https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project
* 就**缓冲区溢出**进行测试
* 就不适当的**错误处理**进行测试
* 就未限制 **URL** 访问进行测试
* 就**目录遍历**进行测试
* 当做出更改时，重复进行内部和独立测试，或者至少每季度测试一次
* 当做出更改时，让独立组织每季度进行一次测试
* 自动测试和手动测试相结合，包括但不限于下列各项：
	+ 互动式内嵌代理程序
	+ **堆**和**堆栈溢出**检测
	+ **验证**不安全性
	+ 用户枚举
	+ **输入验证**
	+ 注明解构或操作的日期
 |
| AS-3.0（续） | 安全编码和系统 |  | * 执行手动及自动测试
* 在网络前端、后端和所有相关的连接执行测试。更正在检测后立即发现的任何有效问题：
	+ 关键：要求立即更正
	+ 高：要求立即更正
	+ 中：在下一个应用程序例行发布时要求更正
	+ 低：倘将在一个相互协定的时间框架内更正，要求获得一个路线图
 |
| AS-3.1 | 每个季度至少执行一次漏洞测试。 | * 使用网络安全行业标准工具
* 当做出更改时，重复进行测试，或者至少每季度测试一次
* 由一家独立组织执行测试
* 更正在检测后立即发现的任何问题
* 在网络前端、后端服务器和所有相关的连接执行测试
 |
| AS-3.2 | 以安全的方式使用 **cookie**（如果需要使用的话） | * 加密 **cookie**（与 **cookie** 哈希运算法相反）
* 使用 **HttpOnly** 设置
* 将 **cookie** 限定于个别应用程序
* 将 **cookie** 限定于个别会话
 |
| AS-3.3 | 验证用户输入和实施安全的**错误处理。** | * 验证所有输入
* 审查所有输入
* 使用安全的错误讯息应对不正确的用户输入，即不泄露恶意用户觉得对于攻击系统有帮助的信息的讯息
 |
| AS-3.4 | 安全编码和系统 | 实施安全的登录程序。 | * 至少登入下列事项：
	+ **输入验证**失败
	+ 输出验证失败
	+ **验证**成功和失败
	+ **授权**（访问控制）失败
	+ **会话管理**失败（例如 cookie 会话识别价值修改）
	+ 应用程序错误
	+ 系统错误和事件
	+ 应用程序和系统启动、关闭、暂停和登录初始化
	+ 使用风险更高的功能（例如管理员和开发商功能）
	+ 法律和其他选择加入
	+ 所有内容和客户文件/文件事件
	+ 任何类型的密钥处理
	+ 系统级别目标的设立和删除
	+ **地理位置**锁定
* 登录下列特征：
	+ 何时（例如日期和时间）
	+ 何地（例如应用程序标识符、应用程序地址、服务、**地理位置**、入口点以及代码位置）
	+ 谁（例如源地址或用户身份）
	+ 什么（例如事件类型、严重程度、事件旗帜和描述、成功或失败指示）
 |
| AS-3.4（续） | 安全编码和系统 |  | * 保护审计记录免被篡改：
	+ 静态：
* 确立篡改检测
* 尽快存储或复制记录到只读媒体
* 记录和监控对记录的所有访问
* 经常审核记录特权
	+ 传输中：
* 使用安全的传输协议
* 考虑验证事件数据的来源
* 验证传输中的数据实际上被加密
* 记录至少保留两年
 |
| AS-3.5 | 实施 **SIEM**（安全信息事件管理系统），以汇总和分析分散的记录。 | * 实施 **SIEM**，包括以下各项：
	+ 集中式事件记录数据存储库/服务器、系统、应用程序和基础设施设备的事件记录集合
	+ 多个独立的安全事件与一个单一的相关安全事件的自动相关性
	+ 发出警报，通过使用仪表板和/或电子邮件，通知安全团队紧迫的问题
	+ 关于记录的文件完整性监控或更改检测软件，以确保现有记录数据不能在被更改的情况下不发出警报（但新增数据不发出警报）
	+ 发出警报，显示从两个不同的地点同时登录同一个帐户
 |
| AS-3.6 | 加密静态的所有内容和客户端数据。 | * 使用 **AES**-256 或更高
* 加密移动应用程序上的所有内容
 |
| AS-3.7 | 安全编码和系统  | 加密正在传输中的所有内容和客户端数据。 | * 考虑以下方面：
	+ 使用**传输层安全性 (TLS)：**
* 使用 **TLS**，了解所有登录页面和所有已验证的页面
* 在传输敏感性内容时使用 **TLS**
* 不为安全的内容提供非 **TLS** 页面
* 仅支持安全度高的协议：**TLS**1.0、**TLS**1.1 及 **TLS** 1.2
* 支持 **TLS**-PSK 和 **TLS**-SRP，以进行相互**验证**
* 使用 **HTTP 严格传输安全性**
* 仅支持安全的重新交涉
	+ 实施证书：
* 为申请的用户基础使用适当的凭证授权
* 在凭证中使用完全合格的名称
* 使用支持规定的域名的凭证
* 不使用万用字元凭证
* 在凭证中不使用 **RFC 1918**（私人）位址
* 总是提供所有必需的凭证
* 使用安全度高的密钥以及保护这些密钥
	+ 防止敏感性数据的缓存
	+ 停用压缩
	+ 从 **URL** 中删掉敏感性数据
 |
| AS-3.8 | 安全编码和系统 | 实施安全**会话管理控制。** | * 安全地管理会话：
	+ 使用安全会话名称，该名称未披露不必要的详情，比如用户名/ID、令牌或用于编程语言或网络应用程序的技术
	+ 使用足够长的会话 ID，以防止强力攻击
	+ 使用无法预测的随机会话 ID
	+ 尽可能使用严格的**会话管理**
	+ 在处理任何无效会话 ID 之前，先进行验证和筛选
	+ 在特权等级发生任何变更后，重新获得会话 ID
	+ 限制会话 ID 交换机制（如 **cookie** 或 **URL** 参数）
	+ 就每个会话实现空闲超时
	+ 就每个会话设置强制过期超时
	+ 纳入手动会话过期（如注销按钮）。在发生网络浏览器窗口关闭事件时，强行进行会话注销
	+ 尽可能避免网站内容缓存
	+ 即使另行要求缓存，也不要缓存会话 ID
	+ 如果用户共享同一台计算机或设备，利用初始登录超时
	+ 不允许同一个用户名/用户 ID 同时进行多个会话
	+ 禁用浏览器交叉表会话
 |
| AS-3.8（续） | 安全编码和系统 |  | * 如果使用 cookie，应安全地管理 cookie：
	+ 使用 **cookie** 的“Secure”属性
	+ 使用 **cookie** 的“**HttpOnly**”属性
	+ 使用 **cookie** 的“Domain”属性
	+ 使用 **cookie** 的“Path”属性
	+ 使用 **cookie** 的非永久属性（如“Expires”、“Max-Age”）
	+ 避免对相同应用程序内的不同路径或域范围使用相同的 cookie 名称
 |
| AS-3.9 | 实施控制以防止 **SQL 攻击。** | * 使用已准备的语句
* 使用存储过程
* 转义所有用户提供的输入
* 将在相关环境中分配给每个数据库帐户的特权最小化
* 使用**白名单**验证输入
 |
| AS-3.10 | 实施控制，以防止未经验证的 **URL** 重定向和转发。 | * 避免使用重定向和转发
* 如果必须使用重定向，则不允许用户输入 **URL**
* 如果无法避免用户输入，则确保所提供的 URL 是有效的
* 如果必须允许 **URL** 输入，则使用**白名单**整理输入
 |
| AS-3.11 | 如可能，实施控制以防止来自匿名网络（如 **Tor**、**Freenet**、**Netshade**）的连接。 | * 如果用户的 **IP 地址**是匿名的，拒绝与应用程序任何部分的所有连接（如可能）
 |
| AS-3.12 | 实施控制以防止泄漏 **IP 地址**。 | * 防止向第三方应用程序（如社交媒体）泄漏用户的 **IP 地址**
 |
| AS-3.13 | 安全编码和系统 | 实施控制以防止 XSS（**跨站脚本**）。 | * 除了在允许的位置外，不要插入不可信的数据
* 在将不可信的数据插入 HTML 元素内容之前，先进行 HTML 转义
* 在将不可信的数据插入 HTML 通用属性之前，先进行属性转义
* 在将不可信的数据插入 JavaScript 数据值之前，先进行 JavaScript 转义
* 在将不可信的数据插入 HTML 样式属性值之前，先进行 CSS 转义及严格的验证
* 在将不可信的数据插入 HTML **URL** 参数值之前，先进行 **URL** 转义
* 利用库整理 HTML 标记
* 防止基于 DOM 的 XSS
* 在可能的时候（如未使用 JavaScript 时），使用 **HTTPOnly** cookie 标志
 |
| AS-3.14 | 允许发送者选择就内容纳入基于会话的取证（不可见）**水印**。 | * 正在被流式传输的**水印**内容
* 正在被下载的**水印**内容
* 验证取证**水印**能留在屏幕捕获和不同品质的摄像机中
* 验证取证**水印**能被成功检索及被接收者单独识别
* 定期测试取证**水印**的强度
 |
| AS-3.15 | 安全编码和系统 | 实施正式、已编档的内容/资产生命周期。 | * 就内容/资产纳入：
	+ 制作
	+ 编辑版本
	+ 返回
	+ 存档
	+ 已认证的处置/破坏
	+ 每个阶段的保持期
 |

|  |
| --- |
| 最佳实践云安全指南 |

| **编号** | **安全主题** | **最佳实践** | **实施指南** |
| --- | --- | --- | --- |
| CS-1.0 | 组织与管理  | 必须遵守 MPAA 内容最佳实践通用指南。如果应用程序安全和**云端/分布式环境**指南内有更强有力的控制措施，则以更强有力的政策为准。 | * 适用指南：
	+ MS-1 至 MS-12
	+ PS-1 至 PS-21
	+ DS-1 至 DS-15
 |
| CS-1.1 | 每年至少进行一次第三方安全审计（如 **SSAE 16 第二类**、**SOC 1**、**ISO 27000/27001**、MPAA）。 | * 审计必须根据标准信息安全管理系统框架进行衡量
 |
| CS-1.2 | 记录和实施符合适用于信息安全管理的安全行业框架（如 ISO-27001、ISO-22307、CoBIT）的安全和隐私政策。 |  |
| CS-1.3 | 记录和实施基础设施各个组件（如**虚拟机监控程序**、操作系统、**路由器**、DNS 服务器等）的信息安全基准。 | * 安全基准必须以安全行业标准为基准
* 按季进行测试
 |
| CS-1.4 | 记录和实施符合组织当前的信息安全程序的人员安全程序。 |  |
| CS-1.5 | 要求所有员工、承包商和第三方在完成入职流程时签署保密/不披露协议。 |  |
| CS-1.6 | 组织与管理 | 记录和实施在为第三方卸载功能或服务时用于开展安全**尽职调查**的程序。 | * 文件审核（比如独立审计、日志、相容性、**渗透测试**结果和补救计划）
* 验证安全控制
* 验证所有软件供应商遵守系统/软件开发生命周期 (**SDLC**) 安全的行业标准
 |
| CS-1.7 | 记录和实施业务关键任务的**职责划分**。 | * 当**职责划分**不可行时，记录补偿性控制措施。确保纳入以下各项：
	+ **密钥管理**
	+ 应用程序**变更控制**
	+ 安全配置变更管理
 |
| CS-1.8 | 向客户提供关于他们的内容和数据位置的信息。 | * 提供关于数据传输方式的信息
* 提供关于内容和数据位置/法定司法管辖区的信息
 |
| CS-1.9 | 制定编档程序，用于响应政府或第三方提出的客户端数据要求。 |  |
| CS-1.10 | 就标记、处理和保护含有数据的容器和其他容器，制定政策和程序。 | * 遵守结构化的数据标记标准（比如 **ISO 15489**、Oasis XML Catalog Specification、**CSA** 数据类型指南）
 |
| CS-1.11 | 就安全删除内容/数据（包括已存档和已备份的内容/数据）制定程序。 | * 遵守关于清理敏感内容/数据的所有法律和监管要求
 |
| CS-1.12 | 为客户确定、记录和实施可能将客户端内容/数据从一个物理位置移至另一个物理位置的应用场景。 | * 例如场外备份、业务连续性故障转移、复制
* 在实施前，以书面方式披露所有变动
 |
| CS-1.13 | 组织与管理 | 制定、记录和实施额外的**密钥管理**功能、控制措施、政策和程序。 | * 就客户通过外部/公用网络移动内容/数据，提供加强型**加密**（参见 AS-3.6 和 AS-3.7）
* 每当基础设施组件需要通过公用网络与另一个组件通信时，都使用加强型**加密**。加密平台和相关数据至少使用 **AES**-256 或更高标准
* 就创建、管理和使用密钥**划分职责**
* 确定是否允许员工管理客户端项目的密钥
* 确定是否允许客户生成和控制他们自己的**加密**密钥
* 允许就每个客户甚至每个项目创建唯一的**加密**密钥
* 记录**加密**密钥生命周期每个阶段的所有权
* 记录用于管理**加密**密钥的系统
* 记录关于租户生成的**加密**密钥的政策
* 在网络和**虚拟机监控程序**实例之间进行传输以及加密静态数据时，使用**加密**保护数据和虚拟机映像
* 不要把密钥存储在云端
 |
| CS-1.14 | 就所有政策和程序，对人员进行培训。 | * 确保管理员和数据专员就他们对于安全性和数据完整性的法律责任接受恰当的教育
 |
| CS-1.15 | 制定流程，在对安全/隐私政策做出重大变更后通知客户。 |  |
| CS-1.16 | 组织与管理 | 规划、准备和衡量所需的系统性能，以确保服务级别可接受。 | * 考虑以下方面：
	+ 服务可用性
	+ 服务品质
	+ 产能规划
* 提供持续的性能监控
 |
| CS-1.17 | 制定和维持额外的**事件响应**要求，并且在未经授权而访问系统或内容时，立即通知客户。 | * 发布规则和责任，指明公司和客户在发生安全事件时的责任
* 维持与执法机构进行联络的联络人
* 把自定义客户要求整合到安全响应计划中
* 确保 **SIEM** 允许对单个客户端数据进行粒度分析和粒度预警
* 确保**事件响应**计划遵守监管链管理流程和控制措施
* 确保**事件响应**功能包括使用法律允许的取证数据收集和分析
* 在不冻结其他客户端数据的情况下，能够为特定客户提供诉讼保留（从一个特定时间点开始冻结数据）
* 在生成数据响应法律传票时，能够强制进行和证明租户数据分离
* 确定关于将与客户分享哪些安全事件数据（如有）的政策
* 确定将事件告知客户的通知标准和流程
 |

| **编号** | **安全主题** | **最佳实践** | **实施指南** |
| --- | --- | --- | --- |
| CS-2.0 | 操作 | 保护数据中心公用设施服务和环境状况。 | * 监控
* 维持
* 至少按年进行测试
 |
| CS-2.1 | 确保数据中心有恰当的外围和物理安全控制措施。 | * 针对损坏（比如自然原因、自然灾害和蓄意攻击）提供物理保护
* 就预期的自然或人为灾害提供应对措施
* 不使用位于高影响力环境风险（洪灾、龙卷风、地震、飓风、地缘政治不稳定性等）发生概率/发生率高的地方的数据中心
 |
| CS-2.2 | 制定、记录和维持业务连续性计划的额外要求。 | * 针对公用设施服务中断提供保护
* 至少按季测试备份、恢复和冗余机制
* 提供备份和恢复选项，确保还原个别客户的内容和数据
* 就所有重要资产维持完整库存
* 就所有重要供应商/业务关系维持完整库存
 |
| CS-2.3 | 制定、记录和维持额外的变更和配置控制措施。 | * 实施控制措施，以限制和监控向系统安装未经授权的软件
* 提供一种功能，通过政策/元数据标记（比如 TXT/TPM、VN-Tag）识别虚拟机
* 提供一种功能，通过政策标记/元数据标记/硬件标记/硬件 ID 识别硬件
 |
| CS-2.4 | 就所有重要资产（包括资产所有权）维持完整库存。 | * 定期对资产进行库存盘点和对帐
 |
| CS-2.5 | 操作 | 就所有重要供应商关系维持库存。 |  |
| CS-2.6 | 与客户、合作伙伴和服务提供商一起制定和维持服务级别协议 (**SLA**)。 | * 至少纳入以下各项：
	+ 所提供的业务关系和服务的范围
	+ 联络人
	+ 客户 **SLA** 性能的持续可见性并进行报告，即运行时间指标和服务级别监控：
* 客户的监控能力
* 关于系统过度订阅（比如网络、存储、内存、I/O 等）的政策
* 就停机时间向客户做出补偿
	+ 信息安全要求。
* 在多租户环境下防止租户之间泄漏数据或故意/意外泄漏的政策
* 关于客户进行第三方漏洞和渗透评估能力的政策
* 事件响应政策
	+ 业务连续性政策，包括关于还原和恢复功能的政策
	+ 在协议届满或终止时，对内容/数据的处理
	+ 关于影响客户的任何第三方或分包商关系的信息
	+ 关于至少按年更新 **SLA** 的政策
	+ 关于支持单点登录 (SSO) 的政策
	+ 考虑以下方面：
* 安全违规行为报告要求
* 审计和检查处所的权利
 |

| **编号** | **安全主题** | **最佳实践** | **实施指南** |
| --- | --- | --- | --- |
| CS-3.0 | 数据安全  | 实施一个流程，以一种在发生安全事件时能轻松从平台导出用于分析的格式，向客户提供出于正当理由而要求的所有相关日志。 | * 使用 **AES**-128 位**加密**或更好的加密标准，传输审计记录
 |
| CS-3.1 | 考虑提供相关功能，把系统地理位置用作额外的**身份验证**因素。 |   |
| CS-3.2 | 如有要求，提供相关功能，以控制客户端内容/数据存储的物理位置/地域。 | * 让客户能根据他们的内容/数据的地理位置做出决策
* 允许客户指定他们的数据可以遍历到哪些地理位置/从哪些地理位置遍历（根据存储和访问数据的位置，涵盖法定司法管辖考虑因素）
* 确保客户端内容/数据不会迁移至指定的地理边界以外
 |
| CS-3.3 | 制定程序，以确保非生产数据不被复制到生产环境。 | * 将非生产数据与生产数据分开
 |
| CS-3.4 | 制定、记录和实施已公布的程序，用于退出与客户达成的服务安排，包括确保在客户合同终止后，整理客户端内容/数据的所有计算系统。 | * 利用使内容/数据还原变得不可能的擦除解决方案或破坏流程（比如物理破坏、消磁/加密擦除、吊销许可证）
* 制定重复使用设备的政策
 |
| CS-3.5 | 制定和记录用于安全处理设备的政策和程序，有关设备按资产类型分类且在组织处所外部使用 | * 参照**美国国防部 5220.22-M** 的数字粉碎和消磁标准
 |
| CS-3.6 | 数据安全  | 执行同步时间服务协议（例如 NTP），确保所有系统均有共同的时间参照物。 | * 考虑实施至少两个独立的时间源
 |
| CS-3.7 | 设计和配置网络和虚拟环境，以限制和监控可信和不可信的连接之间的流量。 | * 至少按年审核这些配置
* 记录整个基础设施
* 定期更新所有文件
* 定期审核网络内安全域/区域之间允许的访问/连接
 |
| CS-3.8 | 设计、开发和部署多租户应用程序、系统和组件，以便恰当分隔客户端内容和数据。 | * 纳入数据管理政策和程序，以涵盖以下几方面：
	+ 篡改审计
	+ 软件完整性功能，以识别对租户数据的未授权访问
 |
| CS-3.9 | 在向/从虚拟服务器迁移物理服务器、应用程序和内容数据时，使用安全和加密的通信信道。 |  |
| CS-3.10 | 实施技术措施和应用深度防御技术（比如深度数据包分析、流量限制、黑洞），用于检测和及时回应与不寻常的入口/出口流量模式有关且基于网络的攻击（比如 NAC 欺骗和 ARP 中毒攻击和/或 DDOS 攻击）。 |  |
| CS-3.11 | 数据安全 | 制定和记录控制措施，保护虚拟环境。 | * 限制和监控对能管理虚拟分区的公用设施的使用
* 建立一个系统，检测直接针对虚拟基础设施的攻击（例如填充、蓝色药丸、超级跳转 (hyper jumping)）
* 实施技术控制措施，以阻止虚拟基础设施攻击
* 控制对虚拟机映像做出的变更，而不论它们处于何种运行状态
* 根据最少特权原则，限制所有**虚拟机监控程序**管理功能或管理控制台，并通过额外的技术控制措施（比如多因素**身份验证**）提供支持
* 提供一种功能，通过政策标记或元数据（比如标记可用来限制来宾操作系统在错误的国家启动/实例化/传输数据）识别虚拟机
 |

|  |
| --- |
| 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。 |
| **敏捷**  | 敏捷软件开发是一组软件开发方法，当中的要求和解决方案通过自组织、跨职能团队之间的合作不断演变。它促进适应性计划、进化式开发、提前交付、持续改善，并且鼓励快速灵活地响应变更。 |
| **Android 设备管理器** | 一种允许用户远程跟踪、定位和擦除他们的 Android 设备的组件。 |
| **应用程序** | 应用程序软件（*应用程序*）是一套计算机程序，旨在允许用户执行一组协调功能、任务或活动。应用程序软件无法自行运行，而是依靠系统软件来运行。 |
| **身份验证** | 确认单项数据（多项数据）或实体属性真实性的行为。身份验证与身份证明不同，身份证明是指说明或另行表明意在证明某人或某事身份声明的行动，而身份验证则是实际确认该身份的过程。身份验证通常涉及验证至少一种身份证明形式的有效性。 |
| **授权** | 授权是指一种功能，这种功能指明对于与一般信息安全和计算机安全及特殊的访问控制有关的资源的**访问权限**。更正式地讲，“授权”就是界定访问政策。 |
| **Beta 测试** | Beta 测试发生在 alpha 测试之后，可被视为一种外部用户验收测试形式。软件版本（被称为 beta 版）向编程团队外部有限的受众（被称为 beta 版测试人员）发布。向一群人发布软件，以便进一步测试能确保产品几乎没有故障或错误。 |
| **黑盒测试** | 黑盒测试一种软件测试方法，它检查应用程序的功能，而不检查应用程序的内部结构或工作。这种方法几乎可以用于各种级别的软件测试：单元、整体、系统和验收。 |
| **错误跟踪** | 错误跟踪系统或缺陷跟踪系统是一种软件应用程序，它持续跟踪软件开发项目中已报告的软件错误。 |
| **缓冲区溢出** | 在计算机安全和编程中，缓冲区溢出或缓冲区超限是指在把数据写入缓冲区时，程序溢出缓冲区边界及覆盖相邻内存的一种异常现象。这是违反内存安全的一种特殊情况。 |
| **CAPTCHA** | **CAPTCHA**（“全自动区分计算机和人类的公开图灵测试”(**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) 的首字母缩写）是一种用于计算的挑战响应测试，可以确定用户是否为人类。 |
| **变更控制** | 质量管理系统 (QMS) 和信息技术 (IT) 系统内的变更控制是一种正式的流程，被用来确保对产品或系统的变更以一种受控和协调的方式引入。 |
| **云端/分布式环境** | 云计算以计算机资源的效用和消费模式为基础。云计算可能涉及在云端内执行和通过能连接互联网的设备操作的应用程序软件。云计算提供以下三类服务：1) 基础设施即服务 (IAAS)、2) 平台即服务 (PAAS) 和 3) 软件即服务 (SAAS)。IAAS 包括虚拟机、服务器和/或数据存储。PAAS 包括数据库、开发环境和网络服务器。SAAS 包括电子邮件和虚拟桌面等应用程序。云可分类为公有云、私有云和混合云。公有云向公众提供服务。私有云仅可供单个组织使用。混合云拥有两种或以上截然不同而又彼此联系的云（比如私有云和公有云）。 |
| **Cookie** | **身份验证** cookie 是网络服务器用来确定用户是否登录帐户的最常见方法。若没有这种机制，网站就不会知道是应该发送包含敏感信息的页面，还是应该要求用户通过登录来验证他们自己的身份。**身份验证** cookie 的安全性通常取决于发布网站的安全性、用户网络浏览器以及 cookie 数据是否加密。 |
| **跨站脚本** | 跨站脚本 (XSS) 是一种常见于网络应用程序的电脑安全漏洞。XSS 允许攻击者将客户端脚本注入到其他用户观查看的网页上。 |
| **CSA** | 云安全联盟是 (CSA) 一家非营利组织，其宗旨是“促进云计算环境下提供安全保障所采用的最佳实践，提供利用云计算来帮助所有其他计算形式的教育”。 |
| **缺陷修复** | 在代码迁移到制作前，修复软件测试程序中发现的任何缺陷。 |
| **拒绝服务攻击** | 在计算中，拒绝服务 (DoS) 或分布式拒绝服务 (DDoS) 攻击企图使机器或网络资源停止向其目标用户提供服务。 |
| **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。 |
| **目录遍历** | 目录遍历（或路径遍历）[利用](http://en.wikipedia.org/wiki/Security_exploit)用户提供的输入文件名的安全验证/清洁处理不足的漏洞，使代表“遍历父目录”的字符绕过安全验证访问文件 API。该攻击的目标是命令应用程序访问受限访问的[计算机文件](http://en.wikipedia.org/wiki/Computer_file)。该攻击利用安全漏洞（软件按原本的设计运作）而不是利用代码中的错误。目录遍历亦被称为 ../（点点斜杠）攻击、[directory](http://en.wikipedia.org/wiki/Directory_%28file_systems%29) climbing 和 backtracking。该攻击的某些形式也是[标准化](http://en.wikipedia.org/wiki/Canonicalization)攻击。 |
| **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。 |
| **加密** | 将数据转换成未授权的人员无法轻易理解的密码文本。 |
| **错误处理**  | 错误或异常处理是对计算期间所发生的*异常情况*做出响应的流程，异常情况指需要特殊处理的反常或异常情况 — 通常会改变程序运行的正常流程。错误处理是由专门的编程语言结构或计算机硬件机制所提供。 |
| **查找我的 iPhone** | 查找我的 iPhone（亦被称为在 [SpringBoard](http://en.wikipedia.org/wiki/SpringBoard) 上查找 iPhone，以及专门针对其他设备的应用程序，例如查找我的iPad、查找我的 iPod 或查找我的 Mac）是一款由 Apple Inc. 提供的应用程序及服务，允许远程定位跟踪 iOS 设备和 Mac 电脑。 |
| **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。 |
| **格式错误** | 不受控制的格式字符串是一种可用于安全漏洞的软件漏洞。格式字符串可被用于使程序崩溃或执行有害代码。 |
| **Freenet** | Freenet 是一个点对点的平台，采用分散的分布式数据存储保存和传递信息。Freenet 拥有一套免费软件，用于在网络上发布信息和相互沟通。 |
| **模糊测试** | 模糊测试或 fuzzing 是一种自动或半自动软件测试技术，通过向电脑程序输入无效、非预期或随机数据来检测漏洞。 |
| **地理位置** | 地理位置是手机或连接互联网的电脑终端等物体的现实世界地理位置的标识。 |
| **堆溢出** | 堆溢出是一种发生在堆数据区域的**缓冲区溢出**。堆溢出可以不同方式用于基于堆栈溢出的攻击。堆的内存由应用程序在运行时间动态分配，通常包含程序数据。通过以特定的方式损坏此数据，致使应用程序覆盖链接列表指针等内部结构来进行攻击。标准的堆溢出手法是覆盖动态内存分配链路（例如内存分配元数据），并利用生成交换指针覆盖程序函数指针。 |
| **HTTPOnly** | HttpOnly cookie 仅可在通过 HTTP（或 **HTTPS**）传输时使用，其无法通过非 HTTP API（例如 JavaScript）使用。这种限制缓解了（但并未消除）通过**跨站脚本** (XSS) 偷窃会话 cookie 的威胁。大多数现代浏览器支持 HttpOnly cookie。 |
| **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。 |
| **HTTP 严格传输安全协议** | HTTP 严格传输安全协议 (HSTS) 是一种网络安全政策机制，对于防止 **HTTPS** 网站受到降级攻击是必要的，其极大地简化了对 cookie 劫持的保护措施。HTTP 严格传输安全协议允许网络服务器声明网络浏览器（或其他合规用户代理）只能使用安全 **HTTPS** 连接，概不得通过不安全的 HTTP 协议与其交互。 |
| **虚拟机监控程序** | 虚拟机监控程序 (VMM) 是一种创建并运行虚拟机的计算机软件、固件或硬件。 |
| **IAM** | 虽然标识管理本身属于 IT 安全范畴，术语“标识管理”(IdM) 及“标识和访问管理”（或 IAM）在标识和访问管理领域可交换使用。标识管理 (IdM) 描述了系统和企业范围内或跨系统和企业范围的个别负责人、其**身份验证**、**授权**及特权，旨在提高安全性和生产率的同时降低成本、减少停机时间和重复性任务。 |
| **IMEI** | 国际移动设备标识或 IMEI 是识别 3GPP（即 GSM、UMTS 和 LTE）和 [iDEN](http://en.wikipedia.org/wiki/IDEN) 手机以及某些卫星电话的唯一号码。IMEI 一般印刷于手机电池盒的内侧，但通过在拨号盘上输入 **\*#06#** 也可显示于大多数手机的屏幕上，或与其他系统信息一起显示于智能手机操作系统的设置菜单中。 |
| **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、服务器和工作站等。 |
| **输入验证** | 输入验证或数据验证是确保程序在清洁、准确和有用的数据上运作的流程。输入验证利用通常称为“验证规则”、“验证约束”或“检验例程”的惯例检查输入系统的数据的准确性、意义性和安全性。 |
| **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）。 |
| **ISO/IEC 12207** | ISO/IEC 12207 *系统和软件工程 — 软件生命周期过程*是软件生命周期过程国际标准。其旨在成为界定开发和维护软件所需的所有任务的标准。 |
| **ISO 15489** | 一项题为：“信息和文件 – 记录管理”的国际标准。 |
| **ISO 27000/27001** | ISO/IEC 27000 是一项题为：*信息技术 — 安全技术 — 信息安全管理系统 — 概述和词汇表*的国际标准。ISO 27001:2013 是一项题为：“信息技术 — 安全技术 — 信息安全管理系统 — 要求”的信息安全标准。 |
| **ISO 27002** | ISO/IEC 27002 是国际标准组织 (ISO) 和国际电工委员会 (IEC) 发布的一项题为*信息技术 – 安全技术 – 信息安全管理实践守则*的信息安全标准。 |
| **密钥管理** | 制作、分配、存储和注销用来访问加密内容的**密钥**。 |
| **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** | 媒体访问控制地址（MAC 地址）是分配至各网络接口用于在物理网段上通信的唯一标识符。MAC 地址可用于大多数 IEEE 802 网络技术（包括以太网和 [WiFi](http://en.wikipedia.org/wiki/WiFi)）的网络地址。逻辑上，MAC 地址可用于 OSI 参考模型的媒体访问控制子层协议。 |
| **MEID**  | 移动设备识别码 (MEID) 是识别 CDMA 移动站设备实物的全球唯一号码。该号码的格式由 3GPP2 报告 S.R0048 界定，但在实践中，其可被视为 IMEI，但以十六进制数字表示。 |
| **移动设备管理** | 移动设备管理 (MDM) 是管理移动设备（例如智能手机、平板电脑、笔记本电脑和台式电脑）的行业术语。MDM 通常采用具有管理特定供应商移动设备功能的第三方产品实施。 |
| **多因素身份验证** | 多因素**身份验证** (MFA) 是一种电脑访问控制方法，要求用户成功进行若干独立的**身份验证**步骤通过验证。 |
| **Netshade** | NetShade 是 Mac OS X 和 iOS 系统下的一款应用程序，可访问匿名代理及 **VPN** 服务器。 |
| **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。 |
| **NIST 800-53** | NIST Special Publication 800-53《联邦**信息系统**和组织安全和隐私控制》针对所有美国联邦**信息系统**（与国家安全有关的信息系统除外）制定了一系列的安全控制措施。它由美国国家标准与技术研究院出版，该研究院是美国商务部下属的一家非监管机构。 |
| **OWASP** | 开放式**网络应用程序安全**项目 (OWASP) 是一个致力于网络应用程序安全的网上社群。OWASP 社群包括来自世界各地的公司、教育组织和个人。该社群从事创造免费提供的文章、方法、文件、工具和技术。 |
| **PCI 数据安全标准**  | **支付卡行业数据安全标准** (PCI DSS) 是针对处理主要支付卡计划（包括 Visa、MasterCard、American Express、Discover 和 JCB）提供的品牌信用卡的组织制定的专有信息安全标准。不属于主要支付卡计划的私用标记信用卡不纳入 PCI DSS 的范畴。 |
| **渗透测试** | 渗透测试或简式笔测试 (short form pen test) 是对电脑系统的一种攻击，旨在寻找安全漏洞，可能获得访问该系统、其功能和数据的权限。 |
| **快速应用程序开发 (RAD)** | 快速应用程序开发既是用于提述传统软件开发**瀑布**模型的替代方法，亦是提述 James Martin 的快速开发方法名称的一般术语。总之，RAD 软件开发方法不太重视计划任务，而更强调开发。相反，**瀑布**模型强调严格的规范和计划。 |
| **RFC 1918** | 在互联网寻址体系结构中，专用网络是使用私有 **IP 地址**空间、遵循 RFC 1918 就互联网协议第 4 版 (IPv4) 和 RFC 4193 就互联网协议第 6 版 (IPv6) 设定之标准的网络。这些地址常在并非强制使用全球可路由地址，或无法为目的网络应用程序提供全球可路由地址时，用于家庭、办公室和企业局域网 (**LAN**)。 |
| **reCAPTCHA** | reCAPTCHA 最初是由 Luis von Ahn、Ben Maurer、Colin McMillen、David Abraham 和 Manuel Blum 在卡内基梅隆大学的匹兹堡主校区开发的用户对话系统。reCAPTCHA 于 2009 年 9 月被 Google 收购。和 **CAPTCHA** 界面一样，reCAPTCHA 要求用户输入屏幕上扭曲的文本图像中显示的文字。通过显示两个字，它保护网站免受企图访问受限区域的机器人程序攻击，并帮助将书的文本数字化。 |
| **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。 |
| **SANS 关键安全控制措施** | 《有效网络防御的二十个关键安全控制措施》（通常称为共识审计指引或 CAG）是针对电脑安全出版的最佳实践指引。该项目于 2008 年初启动，作为美国国防工业基地中的组织遭遇的极端数据损失的回应。该出版物刊登在 SANS 研究院的网站上。 |
| **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。 |
| **会话管理** | 在计算机科学中，特定的网络交流中的会话是两台或以上的通信设备之间，或电脑和用户之间进行的半永久的交互式信息交换，亦被称为对话、谈话或会议。会话是在某个时间点建立或创建的，然后在某个稍后的时间点消失。 |
| **单点登录** | 单点登录 (SSO) 是一种访问控制属性，可控制对多个相关但独立的软件系统的访问。凭藉此属性，用户可一次登录并获得对所有系统的访问权，而不会被提示重新登录每个系统。单点登录一般使用轻量目录访问协议 (LDAP) 和服务器上存储的 LDAP 数据库实施。 |
| **SLA** | 服务级别协议 (SLA) 是正式界定服务的服务合约的一部分。服务提供商和服务用户之间协定的服务的具体方面 — 范围、质量、责任。SLA 的共同特征是约定的（服务或表现）的交付时间。 |
| **SOC 1 报告** | [SOC 1](http://www.ssae-16.com/ssae-16/soc-1-report/)报告（服务组织控制报告）是关于服务组织的控制措施报告，该服务组织涉及用户实体对财务报告的内部控制。SOC1 报告是您先前认为的标准 SAS70 的报告，包括[第一类](http://www.ssae-16.com/ssae/ssae-16-type-i-report-background-information/)及第二类报告，但属于 **SSAE 16** 指引。 |
| **社会工程** | 在信息安全的背景下，社会工程指利用心理学操纵他人执行行动或泄露机密信息。一种目的在于收集信息、欺诈或系统访问的骗局，与传统的“欺诈”所不同的是，它通常是更复杂的欺诈案的众多步骤之一。 |
| **SQL 攻击** | SQL 攻击是一种代码注入技术，过去经常用于攻击数据驱动的应用程序，将恶意的 SQL 语句插入到查询域达到攻击目的（例如向攻击者泄露数据库内容）。SQL 攻击必须利用应用程序软件的安全漏洞，例如，如果不正确地就嵌入 SQL 语句的字符串转义字符筛选用户输入，或用户输入并非强类型和意外执行。 |
| **SSAE 16 第二类** | **SSAE 16 是对《服务组织控制报告》(SAS70) 当前标准的强化。** |
| **SSL** | 请参阅 **TLS** 了解定义。 |
| **堆栈溢出** | 如果堆栈指针超出堆栈范围就会发生堆栈溢出。调用堆栈可能由有限数量的地址空间组成，该数量通常在程序启动时便已确定。调用堆栈的规模取决于许多因素，包括编程语言、机器结构、多线程和可用内存数量。当程序试图调用超出调用堆栈可用空间的空间时（即当系统试图访问超出调用堆栈范围的内存时，本质上是**缓冲区溢出**），堆栈便会溢出，一般会导致程序崩溃。 |
| **系统／软件开发生命周期 (SDLC)** | 系统开发生命周期由若干明确界定和独特的工作阶段组成，系统工程师和系统开发者凭藉这些工作步骤计划、设计、构建、测试和交付**信息系统**。 |
| **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。 |
| **TLS** | **传输层安全协议** (**TLS**) 及其前身**安全套接层协议** (**SSL**) 是旨在提供电脑网络通信安全的加密协议。它们使用 X.509 证书（因此是非对称加密算法）验证通信对方的身份，并协商一个对称密钥。此会话密钥随后被用于双方之间的加密数据流。 |
| **TOR** | Tor 是可进行匿名通信的免费软件。该软件的名称来源于原始的软件项目名称 *The Onion Router* 的首字母缩写。Tor 通过由逾六千个中继服务器组成的免费、世界范围的自愿者网络引导互联网流量，以避免进行网络监督或流量分析的任何人发现用户的位置和用法。 |
| **二元身份验证** | 二元**身份验证**（亦称为 2FA）通过结合两个不同的组成部分明确识别用户的身份。这些组成部分可能是用户已知的某事、用户拥有的某物或与用户不可分割的重要之事。二元**身份验证**是**多因素身份验证**的一种类型。 |
| **URL** | 统一资源定位符 (URL) 指的是一种资源，它可以指定资源在电脑网络上的位置和检索该资源的机制。URL 是特定类型的统一资源标识符 (URI)，然而许多人互换使用这两个术语。URL 蕴含访问指定资源的方法，而并非每个 URI 都是如此。URL 最常见于参考网页 (http)，但也用于文件传输 (ftp)、电子邮件 (mailto)、数据库访问 (JDBC) 及许多其他应用程序。 |
| **美国国防部 5220.22-M 标准****（NISP 操作手册）** | 美国国防部 (DoD) 5220.22-M 标准或 NISP 操作手册为所有政府承包商制定了关于分类信息的标准程序和要求。NISP 或国家工业安全计划是（美国）管理私营企业访问分类信息需求的名义机构。 |
| **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电脑网络。 |
| **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 |
| **瀑布图** | 瀑布模型是在软件开发过程中使用的一种连续的设计过程，在瀑布模型中，开发进程被视为稳步向下流动（就像瀑布一样），经过概念、启动、分析、设计、构建、测试、生产/实施及维护等阶段。 |
| **水印** | 将信息嵌入到**数字资产**的（可能为）不可逆过程。 |
| **网络应用程序安全**  | 网络应用程序安全是信息安全的一个分支，专门处理网站、网络应用程序和网络服务的安全。 |
| **白名单** | 白名单是获提供特定的特权、服务、流动性、访问权或认可的实体名单或登记册。该名单上的实体将获接受、批准和/或认可。 |
| **广域网 (WAN)** | 覆盖面广（如一家公司）的计算机网络。 |
| **在制品 (WIP)** | 任何被认为不是成品的商品。 |

|  |
| --- |
| 附录 B — MPPA 影片发行渠道定义 |

**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您系列剧集。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 — 常见问题 |

1. **我的服务提供商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. **我的服务提供商需要应用最佳实践“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 对您的提供商进行内容安全评估，我们的评估只需在给定的时间内把您提供商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，我们的服务提供商还需遵循由个别 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 D — 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 |

内容保护的地区和国家办公室的完整联系信息列表位于：[www.mpaa.org/about/around-the-world](file:///C%3A%5CUsers%5CTammy%5CDesktop%5CTMP%5CMotion%20picture%5CQM2%5Cwww.mpaa.org%5Cabout%5Caround-the-world)

**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**