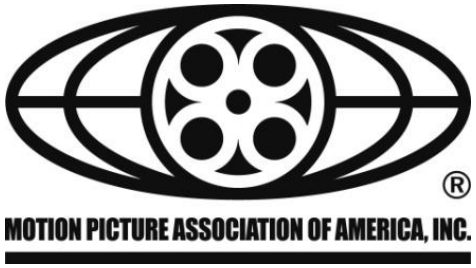


MPAA Content Security Program

CONTENT SECURITY BEST PRACTICES

APPLICATION AND CLOUD/DISTRIBUTED ENVIRONMENT SECURITY GUIDELINES

www.fightfilmtheft.org/en/bestpractices/_piracyBestPractice.asp

Version 1.0

March 17, 2015

DOCUMENT HISTORY

Version	Date	Description	Author
1.0	March 17, 2015	Initial Public Release	MPAA MPAA Member Companies

TABLE OF CONTENTS

I. Best Practices Overview

Introduction

For more than three decades, the Motion Picture Association of America, Inc. (MPAA) has managed site security surveys on behalf of its Member Companies (Members): Walt Disney Studios Motion Pictures; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLC; and Warner Bros. Entertainment Inc.

Starting in 2007, these reviews were performed using a standardized survey model, process and report template. Since then, over 500 facilities have been surveyed in 32 countries.

The MPAA is committed to protecting the rights of those who create entertainment content for audiences around the world. From creative arts to the software industry, more and more people around the globe make their living based on the power of their ideas. This means there is a growing stake in protecting intellectual property rights and recognizing that these safeguards are a cornerstone of a healthy global information economy.

The MPAA Content Security Program's purpose is to strengthen the process by which its Member content is protected during production, post-production, marketing and distribution. This is accomplished by:

- Publishing a set of best practices by facility service outlining standard controls that help to secure Member content;
- Assessing and evaluating content security at third-party partners based on published best practices;
- Reinforcing the importance of securing Member content; and
- Providing a standard survey vehicle for further individual discussions regarding content security between Members and their business partners.

Purpose and Applicability

The purpose of this document is to provide current and future third party vendors engaged by Members with an understanding of general content security expectations and current industry best practices. Decisions regarding the use of vendors by any particular Member are made by each Member solely on a unilateral basis.

Content security best practices are designed to take into consideration the services the facility provides, the type of content the facility handles, and in what release window the facility operates.

Best practices outlined in this document are subject to local, state, regional, federal and country laws or regulations.

Best practices outlined in this document, as well as the industry standards or ISO references contained herein, are subject to change periodically. Best practices are separated into **application** and **cloud/distributed environment** security guidelines. **Vendors must first be assessed by the Best Practices Common Guidelines. In cases where both guidelines apply, the more stringent guidelines take precedence.**

Compliance with best practices is strictly voluntary. This is not an accreditation program.

Exception Process

Where it may not be feasible to meet a best practice, facilities should document why they cannot meet the best practice and implement compensating measures used in place of the best practice. Exceptions should also be communicated directly to the Member.

Questions or Comments

If you have any questions or comments about the best practices, please email: contentsecurity@mpaa.org

II. Provider Overview

The following table describes the typical services offered, type of function, and release window involved with each provider type.

No.	Provider Type	Typical Provider Services	Type of Function	Release Window
1	**Application**	• Application Development • Web Application • Enterprise Resource Planning (ERP) • Information Worker Software • SaaS (Software as a Service)	• Application Development Environment • Varied • Varied • Varied • Varied	• Varied • Varied • Varied • Varied • Varied
2	**Cloud**	• IaaS (Infrastructure as a Service) • PaaS (Platform as a Service) • SaaS (Software as a Service) • Private Cloud • Public Cloud • Hybrid Cloud	• Data Storage, Computing Resources • Application Development Environment • Business Application • Varied • Varied • Varied	• Varied • Varied • Varied • Varied • Varied • Varied

Applicability of Controls

The guidelines in this document (both the Application Security and Cloud Security Guidelines) pertain to all application and cloud vendors.

III. Risk Management

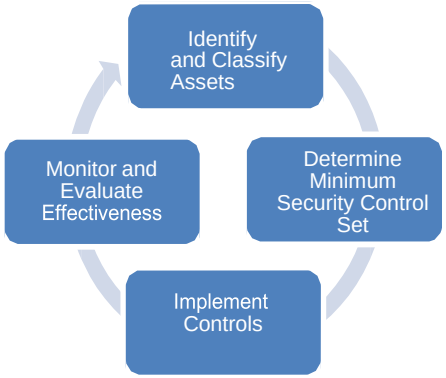
Risk Assessment

Risks should be identified through a **risk assessment**, and appropriate controls should be implemented to decrease risk to an acceptable level and ensure that business objectives are met.

The International Organization for Standardization (ISO) 27000 defines risk as the "combination of the probability of an event and its consequence." For example, what is the probability that content can be stolen from a facility's network and released publicly and what is the business consequence to an organization and the client if this occurs (e.g., contractual breach and/or loss of revenue for that release window). The importance of a robust management system is also highlighted in the ISO 27001 standard that shows how to establish an Information Security Management System (ISMS).

Asset Classification

One way to classify assets at your facility is to follow a four-step process, which is summarized below:



In consultation with the Member (its client), an organization is responsible for determining which client assets require a higher level of security. The following table provides an example of how to classify content:

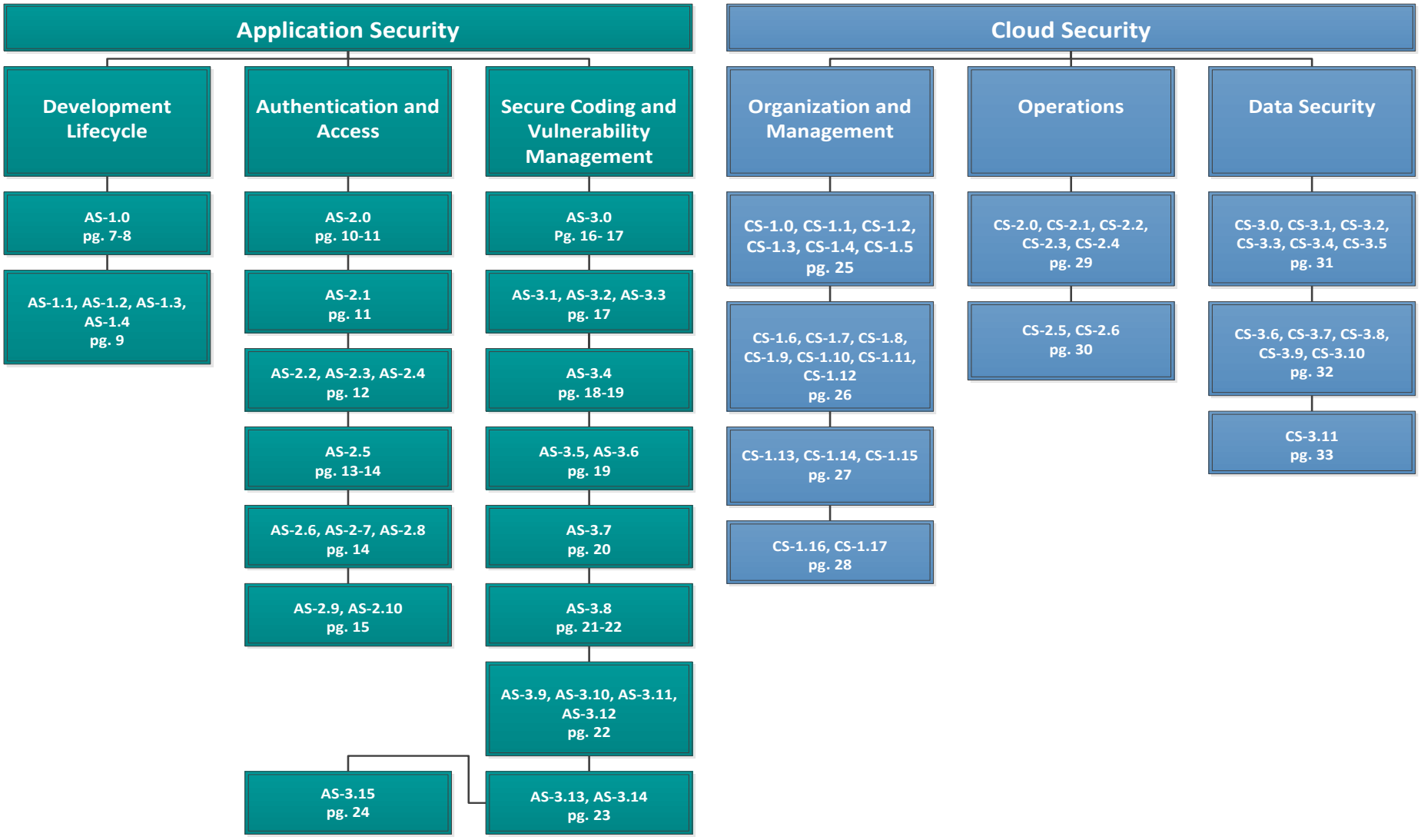
Classification	Description	Examples
High-Security Content	Any content that the organization believes would result in financial loss, negative brand reputation, or serious penalties should the asset be stolen or leaked	• Theft of a blockbuster feature before its first worldwide theatrical release • Theft of home video content before its first worldwide street date • Theft of masters or screeners

Security Controls

The IT Governance Institute defines controls as "the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected." Security controls are typically selected based on the classification of the asset, its value to the organization, and the risk of the asset being leaked or stolen. In order to mitigate identified risks, organizations are encouraged to implement controls commensurate to each specific risk. Such measures should also be evaluated periodically for their design and effectiveness based on the current threat environment. The best practices outlined in this document are based on guidance from the Open Web Application Security Project (**OWASP**), Cloud Security Alliance (**CSA**), **PCI Data Security Standard**, **NIST 800-53**, **SANS Critical Security Controls**, and **ISO 27002**.

IV. Document Organization

Best Practices are organized according to the MPAA Content Security Model, which provides a framework for assessing a provider's ability to protect a client's content. Within the context of this document, the Model comprises security topics across two areas: application security and cloud security. The components of the MPAA Content Security Model are drawn from relevant ISO standards (27001-27002), security standards (i.e., the Open Web Application Security Project [OWASP], Cloud Security Alliance [CSA], PCI Data Security Standard, NIST 800-53, SANS Critical Security Controls) and industry best practices.



V. BEST PRACTICES FORMAT

Best practices are presented for each security topic listed in the MPAA Content Security Model using the following format:

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND VULNERABILITY MANAGEMENT	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

The chart at the top of every page highlights the security area being addressed within the overall MPAA Content Security Model.

No.	Security Topic	Best Practice	Implementation Guidance
AS-2.7	Authentication & Access	Use human verification tools such as **CAPTCHA** or **reCAPTCHA** with web applications	• Use **CAPTCHA** or **reCAPTCHA** to protect against bots

No.

Each best practice is assigned a reference number in the form of XX-Y.Z. XX for the general area, Y for the Security Topic, and Z for the specific control.

Security Topic

Each capability area is comprised of one of more "Security Topics." Each Security Topic is addressed with one or more best practices.

Best Practice

Best practices are outlined for each Security Topic.

Implementation Guidance

Additional considerations, potential implementation steps and examples are provided to help organizations implement the best practices.

Glossary

All terms that are included in the glossary are highlighted in **bold** and defined in Appendix A.

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND VULNERABILITY MANAGEMENT	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

VI. Best Practice Application Security Guidelines

No.	Security Topic	Best Practice	Implementation Guidance

AS-1.0	Development Lifecycle	Build security into the entire **Systems/Software Development Lifecycle** (**SDLC**).	• Consider using industry standard methodologies:
			  ○ **Waterfall**
			  ○ **Rapid Application Development** (**RAD**)
			  ○ **Agile**
			• Refer to **ISO/IEC 12207** for implementation guidance for processes that establish a lifecycle for software and provide a model for the development, acquisition, and configuration of software systems
			• Implement **segregation of duties**:
			  ○ Document all processes and data throughout the requirements/design, construction, testing, release, and maintenance phases including the following:
			  • Program change requests
			  • User acceptance testing and approval
			  • Management approval
			  ○ Separate development and test environments from production environments. Enforce the separation with access controls.
			  ○ Ensure production data is not used in development and test environments.
			• Perform a risk analysis for the systems/software before design begins that includes the following:
			  ○ Threat model including expected vulnerabilities and threats
			  ○ Review by **application** security professional(s)
			  ○ Security and privacy requirements
			  ○ Scope of testing
			• Utilize secure coding standards

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND VULNERABILITY MANAGEMENT	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-1.0 Continued	Development Lifecycle		• Implement **change control:**
			  ○ Log all change migrations into production
			  ○ Restrict access to migrate changes into production
			  ○ Repeat testing when changes are made, or at least on a quarterly basis
			  ○ Prepare back-out procedures according to impact of change
			• Perform Testing:
			  ○ Test security throughout the entire **SDLC** and address vulnerabilities, threats and privacy issues
			  ○ Perform manual as well as automated testing
			  ○ Perform automated security testing including static code analysis and dynamic code analysis
			  ○ Implement controls to detect source code security defects for any outsourced software development activities
			  ○ Remediate any issues
			• Protect details of **application** code from inappropriate use or disclosure:
			  ○ Assign individual administrator accounts for each privileged user to ensure accountability
			  ○ Review all user access on a quarterly basis
			  ○ Remove development, test and/or custom **application** accounts, user IDs, and passwords before **applications** become active or are released to clients
			  ○ Prevent unauthorized access to the **application**/program/source code. Restrict code only to authorized personnel
			  ○ Prevent unauthorized access to tenant **application**, program or object source code, and assure it is restricted to authorized personnel only

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND VULNERABILITY MANAGEMENT	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-1.1	Development Lifecycle	Test security across the entire application and infrastructure.	• Ensure the scope includes the following:
			  ○ Application servers
			  ○ Database servers
			  ○ Server operating systems
			  ○ Virtual server components
			  ○ Web servers, both front end and back end
			  ○ Enterprise architecture components (e.g., service-oriented architectures)
			• Repeat testing when changes are made, or at least on a quarterly basis

AS-1.2		Perform **fuzz testing** and **defect remediation** to discover security loopholes in software, operating systems or networks by massive inputting of random data to the system in an attempt to make it crash (e.g., **buffer overflow**, **cross-site scripting**, **denial of service attacks**, **format bugs**, **SQL injection**).	• Test providing unexpected input • Evaluate how the application reacts • Repeat testing when changes are made, or at least on a quarterly basis
AS-1.3		Perform **bug tracking** and **defect remediation** in conjunction with extensive **black box testing**, **beta testing**, and other proven debugging methods.	• Obtain bug reports for both functional errors and security vulnerabilities • Remediate defects
AS-1.4		Provide training and user guides on additions and changes to the application.	

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-2.0	Authentication & Access	Implement secure **authentication.**	• User names / user IDs:
			  ○ Prohibit the use of duplicate user names / user IDs
			  ○ Prohibit the sharing of user names / user IDs and the simultaneous use of the same user names / user IDs
			  ○ Make user names / user IDs case insensitive
			• Use password controls including:
			  ○ Set a minimum length of at least 8 characters
			  ○ Consider using a maximum password length
			  ○ Enforce strong passwords, using at least 3 of the following 5 rules:
			  • At least 1 upper case character (A-Z)
			  • At least 1 lower case character (a-z)
			  • At least 1 digit (0-9)
			  • At least 1 special character (punctuation or a space)
			  • Not more than 2 identical characters in a row
			  • Maintain password history of at least 10 passwords and deny reuse
			  • Maximum 90 day expiration
			• Lock user account after 5-10 unsuccessful password attempts. Keep the account locked until it is manually unlocked by an administrator.
			• Logoff user automatically after 30 minutes of inactivity. Consider logging off the user or forcing the user to start a new session after 4 hours of being logged in regardless of use or non-use.
			• Store passwords in a secure manner (e.g., not in plain text, transmit passwords only over **TLS**)
			• Require re-**authentication** for sensitive functions
			• Consider the use of **SSL** client **authentication**

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-2.0 Continued	Authentication & Access		• Use a directory service to perform **authentication**
			• Utilize **multi-factor** or **two-factor authentication**:
			  ○ Something you know (account details or passwords)
			  ○ Something you have (token or smartphone)
			  ○ Something you are (biometrics)
			• Consider implementing an Identity and Access Management (**IAM**) system to initiate, capture, record, and manage users and their access permissions in an automated manner to ensure the following:
			  ○ privileges are granted based on interpretation of policy
			  ○ all individuals and services are properly authenticated, authorized and audited

AS-2.1		Register user devices.	• Register devices utilized by application users using, but not limited to the following:
			  ○ Device ID or Hardware ID
			  ○ **IMEI** (International Mobile Equipment Identity) Number or **MEID** (Mobile Equipment Identifier) Number
			  ○ **MAC** (Media Access Control) **address**
			• Check the device being used against a list of known devices for the user during the authentication process
			• Use multifactor **authentication** (e.g., out-of-band delivered one-time password, smartphone PIN) to allow the user to safely register new devices
			• Consider pinning the user account to one or two user devices when practical
			• Consider limiting the number of devices per user (such as a maximum of five devices per user)
			• Prevent users from simultaneously initiating sessions on more than one device

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-2.2	Authentication & Access	Implement secure password recovery.	• Consider the following steps: ○ Gather user-created questions, canned questions or identity data questions (beware of privacy concerns) ○ Define a minimum length for answers to the questions ○ Verify the security questions and answers ○ Design the storage system for the questions and answers ○ Consider having the users periodically review and update the questions and answers ○ Authenticate requests to change questions, possibly using a side channel, such as a pin sent to a smartphone ○ Lock out the user's account immediately and send a token over a side channel ○ Allow the user to change the password in the existing session ○ Test the password recovery process against **social engineering** ○ Verify that the security question bank does not include questions concerning schools, date of birth, maiden name, or any other records that are accessible via internet websites such as LinkedIn, Facebook, etc.
AS-2.3		Follow the principle of least privilege.	• Operate application with a user account, not a privileged account, and with the lowest possible level of permissions • Prohibit the running of the application with system or administrator level permissions
AS-2.4		Implement controls to prevent brute force attacks.	• Lockout user account after a set number of incorrect password attempts; consider using 5-10 as a threshold • Consider keeping the user account locked until it is manually unlocked by an administrator

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-2.5	Authentication & Access	Implement and document a process to secure key / cryptographic storage and ensure ongoing secure management.	• Store only sensitive data that is required to be kept
			• Consider privacy concerns when storing data
			• Support tenant generated **encryption** keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., Identity based **encryption**)
			• Use only strong cryptographic algorithms (e.g., **AES**, RSA public key cryptography, SHA-256 or better)
			• Do not use weak algorithms (e.g., MD5 or SHA1)
			• Ensure randomly generated numbers (used in file names or GUIDs) are cryptographically strong
			• Use only widely accepted implementations of cryptographic algorithms (reference NIST FIPS 140-2)
			• Store the hashed and salted value of passwords, not the passwords themselves.
			• Ensure the cryptographic storage protection remains secure, even if primary controls fail (e.g., always encrypt data at rest)
			• Ensure that secret keys are protected from unauthorized access
			• Define a key lifecycle:
			  ○ Document key handling procedures throughout their lifecycle
			  ○ Document procedures to handle a key compromise
			  ○ Utilize a centralized, automated **key management** approach as opposed to manual key distribution
			  ○ Protect keys in a **vault**
			  ○ Store keys away from the data they are used to encrypt
			  ○ Do not store keys on application servers, web servers, database servers, etc.

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-2.5 Continued	Authentication & Access		○ Recommend the creation of unique **encryption** keys per tenant, and even per project ○ Change keys periodically, at least every 1 to 3 years ○ Rekey data at least every 1 to 3 years ○ **Segregate duties** for creating, managing and using keys ○ Require key custodians to sign a form regarding their related duties and responsibilities ○ Use only secure means to distribute keys (e.g., **TLS**) ○ Use independent keys when multiple keys are required (e.g., do not select a second key that is related to the first key) ○ Prevent unauthorized substitution of keys
AS-2.6		Enable an auto-expiration setting to expire all external links to content after a user-defined time.	• Enable the default setting for link expiration for 24 hours
AS-2.7		Use human verification tools such as **CAPTCHA** or **reCAPTCHA** with web applications.	• Use **CAPTCHA** or **reCAPTCHA** to protect against bots
AS-2.8		Provide clients with the ability to limit the number of times an asset may be downloaded or streamed by a particular user.	

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-2.9	Authentication & Access	Confirm the upload and download of all content and critical assets.	• Send email immediately to content owners, project owners, or project managers whenever content is uploaded, downloaded or viewed
			• Include the following details:
			  ○ Accurate time stamp of all activities
			  ○ Download/stream attempts based on access rules (both successes and failures)
			  ○ Forensic information (e.g., **IP** or **MAC addresses**, **geolocation** information)
			  ○ Number of downloads/streams attempted per asset per user

AS-2.10		Include a brief message on mobile applications to remind users to enable device passwords and to enable remote wipe and device location software.	• Remind users to install location and remote wipe tools such as **Find My iPhone**, **Android Device Manager** • Install, configure and maintain a **mobile device management** system

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-3.0	Secure Coding and Systems	Perform **penetration testing** / **web application security** testing prior to production deployment, and at least quarterly thereafter. Validate vulnerabilities were remediated with a retest.	• Use cybersecurity industry standard tools
			• Test for the **OWASP** Top Ten:
			  ○ A1 Injection (including SQL, OS and LDAP)
			  ○ A2 XSS
			  ○ A3 Weak **authentication** and **session management**
			  ○ A4 Insecure direct object reference
			  ○ A5 Cross site request forgery
			  ○ A6 Security misconfiguration
			  ○ A7 Insufficient cryptographic storage
			  ○ A8 Failure to restrict **URL** access
			  ○ A9 Insufficient transport layer protection
			  ○ A10 Unvalidated redirects and forwards
			  ○ See for updates: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
			• Test for **buffer overflows**
			• Test for improper **error handling**
			• Test for failure to restrict **URL** access
			• Test for **directory traversal**
			• Repeat internal and independent testing when changes are made, or at least on a quarterly basis
			• Have testing performed by an independent organization on a quarterly basis and when changes are made
			• Use a combination of both automated and manual testing, including but not limited to the following:
			  ○ Interactive in-line proxies
			  ○ **Heap** and **stack overflow** detection
			  ○ **Authentication** insecurities
			  ○ User enumeration
			  ○ **Input validation**
			  ○ Date deconstruction or manipulation

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-3.0 Continued	Secure Coding and Systems		• Perform manual as well as automated testing
			• Perform testing on the web front end, the back end and all related connections. Remediate any valid issues found promptly after detection:
			  ○ Critical: Require immediate remediation
			  ○ High: Require immediate remediation
			  ○ Medium: Require remediation in the next regular release of the application
			  ○ Low: Require a roadmap where the remediation will be addressed within a mutually agreeable timeframe

AS-3.1		Perform vulnerability testing at least quarterly.	• Use cybersecurity industry standard tools • Repeat testing when changes are made or at least on a quarterly basis • Have testing performed by an independent organization • Remediate any issues found promptly after detection • Perform testing on the web front end, the back end servers and all related connections
AS-3.2		Utilize **cookies** in a secure manner, if they need to be used	• Encrypt **cookies**, as opposed to hashing **cookies** • Use **HttpOnly** setting • Restrict **cookies** to individual applications • Restrict **cookies** to individual sessions
AS-3.3		Validate user input and implement secure **error handling.**	• Validate all input • Sanitize all input • Respond to incorrect user input with safe error messages, i.e. messages that not give away information that a malicious user might find helpful in attacking the system

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-3.4	Secure Coding and Systems	Implement secure logging procedures.	• Log at least the following events:
			  ○ **Input validation** failures
			  ○ Output validation failures
			  ○ **Authentication** successes and failures
			  ○ **Authorization** (access control) failures
			  ○ **Session management** failures (e.g., cookie session identification value modification)
			  ○ Application errors
			  ○ System errors and events
			  ○ Application and systems start-ups, shut-downs, pausing, and logging initialization
			  ○ Use of higher-risk functionality (e.g., administrator and developer functions)
			  ○ Legal and other opt-ins
			  ○ All content and client folder/file events
			  ○ Key handling of any kind
			  ○ Creation and deletion of system-level objects
			  ○ **Geolocation** blocking
			• Log the following attributes:
			  ○ When (e.g., date and time)
			  ○ Where (e.g., application identifier, application address, service, **geolocation**, entry point, and code location)
			  ○ Who (e.g., source address or user identity)
			  ○ What (e.g., type of event, severity, event flag, and description, success or failure indication)

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

AS-3.4 Continued	Secure Coding and Systems		• Protect the audit logs from tampering:
			  ○ At rest:
			  • Build in tamper detection
			  • Store or copy logs to read-only media asap
			  • Record and monitor all access to the logs
			  • Review log privileges frequently
			  ○ In transit:
			  • Use a secure transmission protocol
			  • Consider verifying the origin of event data
			  • Verify that data in transit is actually being encrypted
			• Retain logs for at least two years

AS-3.5		Implement an **SIEM** (Security Information Event Management System) to aggregate and analyze the disparate logs.	• Implement an **SIEM** including the following:
			  ○ Centralized event log repository for data/event log aggregation from servers, systems, applications and infrastructure devices
			  ○ Automated correlation of multiple isolated security events to a one single, relevant security incident
			  ○ Alerting to notify the security team of immediate issues through the use of a dashboard and/or email
			  ○ File-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data added should not cause an alert)
			  ○ Alerting to indicate concurrent logons of the same account from two different locations

AS-3.6		Encrypt all content and client data at rest.	• Use **AES**-256 or higher • Encrypt all content on mobile applications

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-3.7	Secure Coding and Systems	Encrypt all content and client data in transit.	• Consider the following: ○ Use **Transport Layer Security (TLS):** • Use **TLS** for all login pages and all authenticated pages • Use **TLS** when transmitting sensitive content • Do not provide non-**TLS** pages for secure content • Only support strong protocols: **TLS**1.0, **TLS**1.1 and **TLS** 1.2 • Support **TLS**-PSK and **TLS**-SRP for mutual **authentication** • Use **HTTP strict transport security** • Only support secure renegotiations ○ Implement Certificates: • Use an appropriate certification authority for the application's user base • Use fully qualified names in certificates • Use a certificate that supports required domain names • Do not use wildcard certificates • Do not use **RFC 1918** (private) addresses in certificates • Always provide all needed certificates • Use strong keys and protect them ○ Prevent caching of sensitive data ○ Disable compression ○ Keep sensitive data out of the **URL**

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-3.8	Secure Coding and Systems	Implement controls for secure **session management.**	• Manage sessions securely: ○ Use a secure session name that does not reveal unnecessary details such as user name/ID, token, or the technologies used for programming languages or web applications ○ Use a long enough session ID to prevent brute force attacks ○ Use unpredictable random session ID's ○ Use strict **session management** whenever possible ○ Validate and filter out any invalid session ID's before processing them ○ Renew the session ID after any privilege level change ○ Limit session ID exchange mechanisms (e.g., **cookies** or **URL** parameter) ○ Implement an idle timeout for every session ○ Set mandatory expiration timeouts for every session ○ Include manual session expiration (e.g., logout button). Force session logout on web browser window close events ○ Avoid web content caching whenever possible ○ Never cache session ID's, even if caching is otherwise required ○ Utilize initial login timeouts, in case users share the same computer or device ○ Do not allow multiple simultaneous sessions from the same user name / user ID ○ Disable browser cross-tab sessions

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-3.8 Continued	Secure Coding and Systems		• Manage cookies securely if cookies are used: ○ Use the "Secure" attribute with **cookies** ○ Use the "**HttpOnly**" attribute with **cookies** ○ Use the "Domain" attribute with **cookies** ○ Use the "Path" attribute with **cookies** ○ Use non-persistent attributes (e.g., "Expires", "Max-Age") with **cookies** ○ Avoid using the same cookie names for different paths or domain scopes inside the same application
AS-3.9		Implement controls to prevent **SQL injection.**	• Use prepared statements • Use stored procedures • Escape all user-supplied input • Minimize the privileges assigned to every database account in the environment • Validate input using **whitelisting**
AS-3.10		Implement controls to prevent unvalidated **URL** redirects and forwards.	• Avoid using redirects and forwards • Do not allow the user to input the **URL** if redirects must be used • Ensure the supplied URL is valid if user input cannot be avoided • Sanitize input using **whitelisting** if **URL** input must be allowed
AS-3.11		Implement controls to prevent connections from anonymity networks (e.g., **Tor**, **Freenet**, **Netshade**), if possible.	• Refuse all connections to any part of the application, if the **IP address** of the user is anonymized, if possible
AS-3.12		Implement controls to prevent **IP address** leakage.	• Prevent the leakage of user **IP addresses** to third party applications (e.g., social media)

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-3.13	Secure Coding and Systems	Implement controls to prevent XSS (**Cross-site scripting**).	• Never insert untrusted data, except in allowed locations • HTML Escape before inserting untrusted data into HTML element content • Attribute Escape before inserting untrusted data into HTML common attributes • JavaScript Escape before inserting untrusted data into JavaScript data values • CSS Escape and strictly validate before inserting untrusted data into HTML style property values • **URL** Escape before inserting untrusted data into HTML **URL** parameter values • Sanitize HTML markup with a library • Prevent DOM-based XSS • Use the **HTTPOnly** cookie flag, when possible (e.g., JavaScript is not in use)
AS-3.14		Allow senders the option to include session-based forensic (invisible) **watermarking** for content.	• **Watermark** content that is being streamed • **Watermark** content that is being downloaded • Verify that forensic **watermarks** can survive screen capture and various qualities of camcords • Verify that forensic **watermarks** can be successfully retrieved and individually identified to the recipient • Test the strength of the forensic **watermark** on a regular basis

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
AS-3.15	Secure Coding and Systems	Implement a formal, documented content / asset lifecycle.	• Include for content / assets: ○ Creation ○ Edited versions ○ Return ○ Archival ○ Certified disposal / destruction ○ Retention period for each stage

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

VII. BEST PRACTICE CLOUD SECURITY GUIDELINES

No.	Security Topic	Best Practice	Implementation Guidance
CS-1.0	Organization & Management	Compliance with the MPAA Content Best Practices Common Guidelines is required. Where stronger controls exist within the Application Security and **Cloud/Distributed Environment** Guidelines, the stronger policy will prevail.	• Applicable guidelines: ○ MS-1 through MS-12 ○ PS-1 through PS-21 ○ DS-1 through DS-15
CS-1.1		Perform a third party security audit at least once per year (e.g., **SSAE 16 Type 2**, **SOC 1**, **ISO 27000/27001**, MPAA).	• Audit must measure against a standard Information Security Management System framework
CS-1.2		Document and implement security and privacy policies that are aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO-22307, CoBIT).	
CS-1.3		Document and implement information security baselines for every component of the infrastructure (e.g., **Hypervisors**, operating systems, **routers**, DNS servers, etc.).	• Security baselines must be benchmarked against security industry standards • Test on a quarterly basis
CS-1.4		Document and implement personnel security procedures that align with the organization's current information security procedures.	
CS-1.5		Require all employees, contractors, and third parties to sign confidentiality / non-disclosure agreements when going through the onboarding process.	

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-1.6	Organization & Management	Document and implement procedures for conducting security **due diligence** when offloading functionality or services to a third party.	• Documentation reviews (e.g., independent audits, logs, compliance, **penetration test** results, and remediation plans) • Validation of security controls • Verify that all software suppliers adhere to industry standards for Systems/Software Development Lifecycle (**SDLC**) security
CS-1.7		Document and implement **segregation of duties** for business critical tasks.	• Document compensating controls where **segregation of duties** is not feasible. Be sure to include the following: ○ **Key management** ○ Application **change control** ○ Security configuration change management
CS-1.8		Provide clients with information regarding locations for their content and data.	• Provide information on how data is transported • Provide information on content and data location / legal jurisdictions
CS-1.9		Develop a documented procedure for responding to requests for client data from governments or third parties.	
CS-1.10		Establish policies and procedures for labeling, handling, and securing containers that contain data and other containers.	• Follow a structured data-labeling standard (e.g., **ISO 15489**, Oasis XML Catalog Specification, **CSA** data type guidance)
CS-1.11		Establish procedures for the secure deletion of content/data, including archived and backed-up content/data.	• Comply with all legal and regulatory requirements for scrubbing of sensitive content/data
CS-1.12		Establish, document and implement scenarios to clients in which client content/data may be moved from one physical location to another.	• E.g., offsite backups, business continuity failovers, replication • Disclose all movements in writing prior to implementation

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-1.13	Organization & Management	Establish, document and implement additional **key management** features, controls, policies and procedures.	• Provide strong **encryption** (see AS-3.6 and AS-3.7) for clients' move content/data through external/public networks • Use strong **encryption** any time infrastructure components need to communicate with one another via public networks. Encrypt platforms and related data using at least **AES**-256 or higher • **Segregate duties** for creating, managing and using keys • Determine if employees are allowed to manage the keys for client projects • Determine if clients are allowed to generate and control their own **encryption** keys • Allow for the creation of unique **encryption** keys per client and even per project • Document ownership for each stage of the lifecycle of **encryption** keys • Document systems used to manage **encryption** keys • Document the policy regarding tenant-generated **encryption** keys • Use **encryption** to protect data and virtual machine images during transport across and between networks and **hypervisor** instances, as well as encrypting data at rest • Do not store keys in the cloud
CS-1.14		Train personnel regarding all policies and procedures.	• Ensure administrators and data stewards are properly educated on their legal responsibilities with regard to security and data integrity
CS-1.15		Establish a process to notify clients when material changes are made to security/privacy policies.	

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance

CS-1.16	Organization & Management	Plan, prepare and measure the required system performance to ensure acceptable service levels.	• Consider the following:
			  ○ Availability of service
			  ○ Quality of service
			  ○ Capacity planning
			• Provide continuous performance monitoring

CS-1.17		Develop and maintain additional requirements for **incident response** and immediate notification to the client in the event of any unauthorized access to systems or content.	• Publish rules and responsibilities specifying company responsibilities from client responsibilities in the event of a security incident • Maintain points of contact with law enforcement • Integrate customized client requirements into the security response plan • Ensure the **SIEM** allows for granular analysis of and granular alerting of individual client data • Ensure the **incident response** plan complies with chain-of-custody management processes and controls • Ensure the **incident response** capability includes the use of legally admissible forensic data collection and analysis • Have the capability to support litigation holds (freeze of data from a specific point in time) for a specific client without freezing other client data • Have the capability to enforce and attest to tenant data separation when producing data in response to legal subpoenas • Determine the policy as to which security incident data, if any, will be shared with clients • Determine the notification criteria and process to inform clients of an incident

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-2.0	Operations	Secure datacenter utilities services and environmental conditions.	• Monitor • Maintain • Test at least annually
CS-2.1		Ensure the data center has appropriate perimeter and physical security controls.	• Provide physical protection against damage (e.g., natural causes, natural disasters, and deliberate attacks) • Provide countermeasures to anticipated natural or man-made disasters • Do not use data centers located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, geopolitical instability, etc.)
CS-2.2		Develop, document and maintain additional requirements for business continuity planning.	• Provide protection against utility service outages • Test backup, recovery and redundancy mechanisms at least quarterly • Provide backup and recovery options to ensure the content and data of an individual client may be restored • Maintain a complete inventory of all critical assets • Maintain a complete inventory of all critical supplier/business relationships
CS-2.3		Develop, document and maintain additional change and configuration controls.	• Implement controls to restrict and monitor the installation of unauthorized software onto systems • Provide a capability to identify virtual machines via policy/metatags (e.g., TXT/TPM, VN-Tag) • Provide a capability to identify hardware via policy tags/metadata/hardware tags/hardware ID’s
CS-2.4		Maintain a complete inventory of all critical assets, including ownership of the asset.	• Conduct periodic inventory counts and reconciliation of assets

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-2.5	Operations	Maintain an inventory of all critical supplier relationships.	
CS-2.6		Develop and maintain service level agreements (**SLA**'s) with clients, partners, and service providers.	• Include the following at a minimum: ○ Scope of business relationship and services offered ○ Points of contact ○ Ongoing visibility and reporting on client **SLA** performance, i.e. uptime metrics and service level monitoring: • Client's ability to monitor • Policy on system oversubscription (e.g., network, storage, memory, I/O, etc.) • Reimbursement to client for downtime ○ Information security requirements. • Policy to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment • Policy on clients' ability to perform third party vulnerability and penetration assessments • Incident response policy ○ Business continuity policy, including policy on restore and recovery capabilities ○ Treatment of content/data at expiration or termination of agreement ○ Information on any third party or sub-contractor relationships that affect the clients ○ Policy for updating of the **SLA**s on at least an annual basis ○ Policy on support for single sign on (SSO) ○ Consider the following: • Security breach reporting requirements • Right to audit and inspect premises

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-3.0	Data Security	Implement a process to provide all relevant logs requested for good cause to clients in a format that can be easily exported from the platform for analysis in the event of a security incident.	• Transport audit logs using **AES**-128 bit **encryption** or better
CS-3.1		Consider providing the capability to use system geographic location as an additional **authentication** factor.	
CS-3.2		Provide the capability to control the physical location/geography of storage of a client's content/data, if requested.	• Provide the ability for clients to decide upon the geographic location of their content/data • Allow clients to specify which geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed) • Ensure that client content/data does not migrate beyond the specified geographic boundaries
CS-3.3		Establish procedures to ensure that non-production data must not be replicated to production environments.	• Segregate non-production data from production data
CS-3.4		Establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/data once the client contract has terminated.	• Utilize a wiping solution or destruction process that renders recovery of content/data impossible (e.g. physical destruction, degaussing/cryptographic wiping, revocation of license) • Develop policies for reuse of equipment
CS-3.5		Establish and document policies and procedures for secure disposal of equipment, categorized by asset type, used outside the organization's premises.	• Reference **U.S. Department of Defense 5220.22-M** for digital shredding and wiping standards

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-3.6	Data Security	Implement a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference.	• Consider implementing at least two independent time sources
CS-3.7		Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections.	• Review these configurations at least annually • Document the entire infrastructure • Regularly update all documentation • Regularly review allowed access/connectivity between security domains/zones within the network

CS-3.8		Design, develop and deploy multi-tenant applications, systems, and components such that client content and data is appropriately segmented.	• Include data management policies and procedures to address the following:
			  ○ A tamper audit
			  ○ Software integrity function to identify unauthorized access to tenant data

CS-3.9		Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/from virtual servers.	
CS-3.10		Implement technical measures and apply defense-in-depth techniques (e.g., deep-packet analysis, traffic throttling, black-holing) for detection and timely response to network-based attacks associated with unusual ingress/egress traffic patterns (e.g., NAC spoofing and ARP poisoning attacks and/or DDOS attacks).	

APPLICATION SECURITY			CLOUD SECURITY		
DEVELOPMENT LIFECYCLE	AUTHENTICATION AND ACCESS	SECURE CODING AND SYSTEMS	ORGANIZATION AND MANAGEMENT	OPERATIONS	DATA SECURITY

No.	Security Topic	Best Practice	Implementation Guidance
CS-3.11	Data Security	Establish and document controls to secure virtualized environments.	• Restrict and monitor the use of utilities that can manage virtual partitions • Implement a system to detect attacks that can target the virtual infrastructure directly (e.g., shimming, blue pill, hyper jumping) • Implement technical controls to block virtual infrastructure attacks • Control changes made to virtual machine images, regardless of their running state • Restrict all **hypervisor** management functions or administrative consoles based upon the principle of least privilege and support this through additional technical controls (e.g., multi-factor **authentication**) • Provide a capability to identify virtual machines via policy tags or metadata (e.g. tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)

APPENDIX A — GLOSSARY

This glossary of basic terms and acronyms are most frequently used and referred to within this publication. These definitions have been taken from relevant ISO standards (27001/27002), security standards (i.e., NIST) and industry best practices. In the best practices guidelines, all terms that are included in this glossary are highlighted in **bold.**

Term or Acronym	Description
Access Rights	Permission to use/modify an object or system.
Advanced Encryption Standard (AES)	A NIST symmetric key **encryption** standard that uses 128-bit blocks and key lengths of 128, 192, or 256 bits.
Agile	Agile software development is a group of software development methods in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, continuous improvement and encourages rapid and flexible response to change.
Android Device Manager	A component that allows users to remotely track, locate and wipe their Android device.
Application	Application software (an *application*) is a set of computer programs designed to permit the user to perform a group of coordinated functions, tasks, or activities. Application software cannot run on itself, but is dependent on system software to execute.

Term or Acronym	Description
Authentication	The act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. Authentication often involves verifying the validity of at least one form of identification.
Authorization	Authorization or authorization is the function of specifying **access rights** to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.
Beta Testing	Beta testing comes after alpha testing and can be considered a form of external user acceptance testing. Versions of the software, known as beta versions, are released to a limited audience outside of the programming team known as beta testers. The software is released to groups of people so that further testing can ensure the product has few faults or bugs.

Term or Acronym	Description
Black Box Testing	Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method can be applied to virtually every level of software testing: unit, integration, system and acceptance.
Bug Tracking	A bug tracking system or defect tracking system is a software application that keeps track of reported software bugs in software development projects.
Buffer Overflow	In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety.
CAPTCHA	A **CAPTCHA** (an acronym for "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part") is a type of challenge-response test used in computing to determine whether or not the user is human.
Change Control	Change control within quality management systems (QMS) and information technology (IT) systems is a formal process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner.

Term or Acronym	Description
Cloud/Distributed Environment	Cloud computing is based on a utility and consumption model for computer resources. Cloud computing can involve application software which is executed within the cloud and operated through Internet enabled devices. Cloud computing provides three types of services as follows: 1) Infrastructure as a service (IAAS), 2) Platform as a service (PAAS), and 3) Software as a service (SAAS). IAAS includes virtual machines, servers, and/or data storage. PAAS includes databases, development environment, and web servers. SAAS includes applications such as email and virtual desktop. Clouds can be classified as public, private or hybrid. Public clouds provide services for the public. Private clouds are only available for a single organization. A hybrid cloud has two or more clouds that are distinct, but bound together (e.g. Private and Public clouds).
Cookies	**Authentication** cookies are the most common method used by web servers to determine whether or not users are logged into an account. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the users to authenticate themselves by logging in. The security of an **authentication** cookie generally depends on the security of the issuing website, the user's web browser and on whether the cookie data is encrypted.

Term or Acronym	Description
Cross-Site Scripting	Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.
CSA	Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to “promote the use of best practices for providing security assurance within Cloud Computing and to provide education on the uses of Cloud Computing to help secure all other forms of computing”.
Defect Remediation	Resolving any defects that were discovered in the software testing process, before the code is migrated to Production.
Denial of Service Attacks	In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.
Digital Asset	Any form of content and/or media that has been formatted into a binary source which includes the right to use it.

Term or Acronym	Description
Directory Traversal	A directory traversal (or path traversal) consists in exploiting insufficient security validation / sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs. The goal of this attack is to order an application to access a computer file that is not intended to be accessible. This attack exploits a lack of security (the software is acting exactly as it is supposed to) as opposed to exploiting a bug in the code. Directory traversal is also known as the ../ (dot dot slash) attack, directory climbing and backtracking. Some forms of this attack are also canonicalization attacks.
Due Diligence	The research or investigation of a potential employee or **third party worker** that is performed before hire to ensure good standing.
Encryption	The conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.
Error Handling	Error or Exception handling is the process of responding to the occurrence, during computation, of *exceptions* – anomalous or exceptional conditions requiring special processing – often changing the normal flow of program execution. It is provided by specialized programming language constructs or computer hardware mechanisms.
Find My iPhone	Find My iPhone (also known as Find iPhone on the SpringBoard and specifically for other devices as Find My iPad, Find My iPod, or Find My Mac) is an app and service provided by Apple Inc. that allows remote location-tracking of iOS devices and Mac computers.

Term or Acronym	Description
Firewall	Gateway that limits access between networks in accordance with local security policy.
Firewall Ruleset	Table of instructions that the **firewall** uses for determining how packets should be routed between source and destination.
FireWire	A high-speed interface that allows data to be transmitted from external devices to a computer.
Format Bugs	Uncontrolled format string is a type of software vulnerability that can be used in security exploits. Format string exploits can be used to crash a program or to execute harmful code.
Freenet	A peer-to-peer platform that uses a decentralized distributed data store to keep and deliver information. It has a suite of free software for publishing and communicating on the Web.
Fuzz Testing	Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program.
Geolocation	Geolocation is the identification of the real-world geographic location of an object, such as a mobile phone or Internet-connected computer terminal.

Term or Acronym	Description
Heap Overflow	A heap overflow is a type of **buffer overflow** that occurs in the heap data area. Heap overflows are exploitable in a different manner to that of stack-based overflows. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc meta data) and uses the resulting pointer exchange to overwrite a program function pointer.
HTTPOnly	HttpOnly cookies can only be used when transmitted via HTTP (or **HTTPS**). They are not accessible through non-HTTP APIs such as JavaScript. This restriction mitigates, but does not eliminate, the threat of session cookie theft via **cross-site scripting** (XSS). HttpOnly cookies are supported by most modern browsers.
HTTPS	A communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.
HTTP Strict Transport Security	HTTP Strict Transport Security (HSTS) is a web security policy mechanism which is necessary to protect secure **HTTPS** websites against downgrade attacks and which greatly simplifies protection against cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure **HTTPS** connections and never via the insecure HTTP protocol.

Term or Acronym	Description
Hypervisor	A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines.
IAM	The terms "Identity Management" (IdM) and "Identity and Access Management" (or IAM) are used interchangeably in the area of Identity access management, while identity management itself falls under the umbrella of IT Security. Identity management (IdM) describes the management of individual principals, their **authentication**, **authorization** and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.
IMEI	The International Mobile Station Equipment Identity or IMEI is a number, usually unique, to identify 3GPP (i.e., GSM, UMTS and LTE) and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering ***#06#** on the dial pad, or alongside other system information in the settings menu on smartphone operating systems.
Incident Response	The detection, analysis and remediation of security incidents.
Information Systems	Any electronic or computer-based system that is used by the facility to process information. **Information systems** include applications, network devices, servers and workstations, among others.

Term or Acronym	Description
Input Validation	Input validation or data validation is the process of ensuring that a program operates on clean, correct and useful data. It uses routines, often called "validation rules", "validation constraints" or "check routines" that check for correctness, meaningfulness and security of data that are input to the system.
IP Address	A numerical identification (logical address) that is assigned to devices participating in a computer network.
ISO/IEC 12207	ISO/IEC 12207 *Systems and software engineering — Software life cycle processes* is an international standard for software lifecycle processes. It aims to be *the* standard that defines all the tasks required for developing and maintaining software.
ISO 15489	An international standard entitled: “Information and documentation – Records management”.
ISO 27000/27001	ISO/IEC 27000 is an international standard entitled: *Information technology — Security techniques — Information security management systems — Overview and vocabulary***.** ISO 27001:2013 is an information security standard entitled: "Information technology— Security techniques — Information security management systems — Requirements".
ISO 27002	ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), titled *Information technology – Security techniques – Code of practice for information security management*.

Term or Acronym	Description
Key Management	The creation, distribution, storage and revocation of **encryption** keys that are used to access encrypted content.
Local Area Network (LAN)	Computer network covering a small physical area (e.g., an office).
MAC Address	A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.
MEID	A mobile equipment identifier (MEID) is a globally unique number identifying a physical piece of CDMA mobile station equipment. The number format is defined by the 3GPP2 report S.R0048, but in practical terms, it can be seen as an IMEI but with hexadecimal digits.
Mobile Device Management	Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.
Multi-Factor Authentication	Multi-factor **authentication** (MFA) is a method of computer access control which a user can pass by successfully presenting several separate **authentication** stages.

Term or Acronym	Description
Netshade	NetShade is an app for Mac OS X and iOS which provides access to anonymous proxy and **VPN** servers.
Network Protocol	Convention or standard that controls or enables the connection, communication and data transfer between computing endpoints.
NIST 800-53	NIST Special Publication 800-53, "Security and Privacy Controls for Federal **Information Systems** and Organizations," provides a catalog of security controls for all U.S. federal **information systems** except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce.
OWASP	Open **Web Application Security** Project (OWASP) is an online community dedicated to web application security. The OWASP community includes corporations, educational organizations and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools and technologies.
PCI Data Security Standard	The **Payment Card Industry Data Security Standard** (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover and JCB. Private label cards, those which aren't part of a major card scheme, are not included in the scope of the PCI DSS.

Term or Acronym	Description
Penetration Testing	A penetration test, or the short form pen test, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.
Rapid Application Development (RAD)	Rapid application development is both a general term used to refer to alternatives to the conventional **waterfall** model of software development as well as the name for James Martin's approach to rapid development. In general, RAD approaches to software development put less emphasis on planning tasks and more emphasis on development. In contrast, the **waterfall** model emphasizes rigorous specification and planning.
RFC 1918	In the Internet addressing architecture, a private network is a network that uses private **IP address** space, following the standards set by RFC 1918 for Internet Protocol Version 4 (IPv4) and RFC 4193 for Internet Protocol Version 6 (IPv6). These addresses are commonly used for home, office and enterprise local area networks (**LAN**s), when globally routable addresses are not mandatory, or are not available for the intended network applications.

Term or Acronym	Description
reCAPTCHA	reCAPTCHA is a user-dialogue system originally developed by Luis von Ahn, Ben Maurer, Colin McMillen, David Abraham and Manuel Blum at Carnegie Mellon University's main Pittsburgh campus. reCAPTCHA was acquired by Google in September 2009. Like the **CAPTCHA** interface, reCAPTCHA asks users to enter words seen in distorted text images onscreen. By presenting two words, it protects websites from bots attempting to access restricted areas and helps digitize the text of books.
Risk Assessment	The identification and prioritization of risks that is performed to identify possible threats to a business.
Risk Management	The identification, analysis and mitigation of risks through **risk assessment** and the implementation of security controls.
Router	Device whose software and hardware are tailored to the tasks of steering and forwarding information.
SANS Critical Security Controls	The Twenty Critical Security Controls for Effective Cyber Defense (commonly called the Consensus Audit Guidelines or CAG) is a publication of best practice guidelines for computer security. The project was initiated early in 2008 as a response to extreme data losses experienced by organizations in the US defense industrial base. The publication can be found on the website of the SANS Institute.

Term or Acronym	Description
Security information and event management (SIEM)	A term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications
Segregation of Duties	A security principle by which no single person should have the ability to complete a task on his own; a principle by which no single person should be responsible for more than one related function.
Session Management	In computer science, in particular networking, a session is a semi-permanent interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user. A session is set up or established at a certain point in time and then torn down at some later point.
Single Sign-On	Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on servers.

Term or Acronym	Description
SLA	A service-level agreement (SLA) is a part of a service contract where a service is formally defined. Particular aspects of the service - scope, quality, responsibilities - are agreed between the service provider and the service user. A common feature of an SLA is a contracted delivery time (of the service or performance).
SOC 1 Report	A SOC 1 Report (Service Organization Controls Report) is a report on Controls at a Service Organization which are relevant to user entities' internal control over financial reporting. The SOC1 Report is what you would have previously considered to be the standard SAS70, complete with a Type I and Type II reports, but falls under the **SSAE 16** guidance.
Social Engineering	Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Term or Acronym	Description
SQL Injection	SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g., to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.
SSAE 16 Type 2	SSAE 16 is an enhancement to the current standard for Reporting on Controls at a Service Organization, the SAS70.
SSL	See **TLS** for a definition.
Stack Overflow	A stack overflow occurs if the stack pointer exceeds the stack bound. The call stack may consist of a limited amount of address space, often determined at the start of the program. The size of the call stack depends on many factors, including the programming language, machine architecture, multi-threading and amount of available memory. When a program attempts to use more space than is available on the call stack (that is, when it attempts to access memory beyond the call stack's bounds, which is essentially a **buffer overflow**), the stack is said to overflow, typically resulting in a program crash.
Systems/Software Development Lifecycle (SDLC)	A systems development life cycle is composed of a number of clearly defined and distinct work phases which are used by systems engineers and systems developers to plan for, design, build, test and deliver **information systems**.
Third Party Worker	Any individual who works for an external company but is hired by the facility to provide services. Third party workers include contractors, freelancers and temporary agencies.
TLS	**Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols designed to provide communications security over a computer network. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating and to negotiate a symmetric key. This session key is then used to encrypt data flowing between the parties.
TOR	Tor is free software for enabling anonymous communication. The name is an acronym derived from the original software project name *The Onion Router*. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.
Two-Factor Authentication	Two-factor **authentication** (also known as 2FA) provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. Two-factor **authentication** is a type of **multi-factor authentication**.

Term or Acronym	Description
URL	A uniform resource locator (URL) is a reference to a resource that specifies the location of the resource on a computer network and a mechanism for retrieving it. A URL is a specific type of uniform resource identifier (URI), although many people use the two terms interchangeably. A URL implies the means to access an indicated resource, which is not true of every URI. URLs occur most commonly to reference web pages (http), but are also used for file transfer (ftp), email (mailto), database access (JDBC) and many other applications.
U.S. Department of Defense 5220.22-M (NISP Operating Manual)	DoD 5220.22-M, or the NISP Operating Manual, establishes the standard procedures and requirements for all government contractors, with regards to classified information. NISP or the National Industrial Security Program, is the nominal authority (in the United States) for managing the needs of private industry to access classified information.
Vault	An area that is dedicated to storing physical media with content.
Virtual Local Area Network (VLAN)	Computer network having the attributes of a **LAN** / Internal Network but not limited to physical location.
Virtual Private Network (VPN)	Computer network that allows users to access another larger network.

Term or Acronym	Description
Waterfall	The waterfall model is a sequential design process, used in software development processes, in which progress is seen as flowing steadily downwards (like a waterfall) through the phases of conception, initiation, analysis, design, construction, testing, production/implementation and maintenance.
Watermarking	The process of (possibly) irreversibly embedding information into a **digital asset**.
Web Application Security	Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services.
Whitelisting	A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. Entities on the list will be accepted, approved and/or recognized.
Wide Area Network (WAN)	Computer network covering a broad area (e.g., a company).
Work in Progress (WIP)	Any good that is not considered to be a final product.

APPENDIX B — MPAA TITLE AND DISTRIBUTION CHANNEL DEFINITIONS

Title Types

<table>
<tr><th>Title Type</th><th>Description</th></tr>
<tr><td>Feature</td><td>A type of work released theatrically or direct to home video or to Internet that includes the following types:
<table>
<tr><th>Feature Type</th><th>Description</th></tr>
<tr><td>Feature Film</td><td>A full length movie.</td></tr>
<tr><td>Short</td><td>A film of length shorter than would be considered a feature film.</td></tr>
<tr><td>Long-Form Non-Feature</td><td>Other works, for example, a documentary.</td></tr>
</table></td></tr>
<tr><td>TV Episodic</td><td>A type of work that is TV, web or mobile related and includes episodes of a season or miniseries. A pilot is also an episode as are other specialized sequences (such as “webisode” or “mobisode”).</td></tr>
<tr><td>TV Non-Episodic</td><td>A type of work that is TV, web, or mobile related, but does not have episodes (e.g., made-for-television movies, sporting events, or news programs).</td></tr>
<tr><td>Promotion / Advertisement</td><td>A type of work that includes:
“Promotion” – Any promotional material associated with media. This includes teasers, trailers, electronic press kits and other materials. Promotion is a special case of ‘Ad’.</td></tr>
</table>

<table>
<tr><th>Title Type</th><th>Description</th></tr>
<tr><td>Ad</td><td>Any form of advertisement including TV commercials, infomercials, public service announcements and promotions not covered by “Promotion.” This does not include movie trailers and teasers even though they might be aired as a TV commercial.</td></tr>
<tr><td>Music</td><td>A type of work that includes ringtone, music videos and other music.</td></tr>
<tr><td>Other</td><td>A type of work that includes:
<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>Excerpt</td><td>An asset that consists primarily of portion or portions of another work or works.</td></tr>
<tr><td>Supplemental</td><td>Material designed to supplement another work. For example, an extra associated with a DVD.</td></tr>
<tr><td>Collection</td><td>A collection of assets not falling into another category. For example, a collection of movies.</td></tr>
<tr><td>Franchise</td><td>A collection or combination of other types, for example, a franchise might include multiple TV shows, or TV shows and movies.</td></tr>
</table></td></tr>
</table>

Distribution Channels

Distribution Channel	Description
Theatrical	A feature film is released exclusively into theaters.
Non-Theatrical	A motion picture is released publicly in any manner other than television, home video or theatrical. It includes the exhibition of a motion picture (i) on airplanes, trains, ships and other common carriers, (ii) in schools, colleges and other educational institutions, libraries, governmental agencies, business and service organizations and clubs, churches and other religious oriented groups, museums, and film societies (including transmission of the exhibition by closed circuit within the immediate area of the origin of such exhibition), and (iii) in permanent or temporary military installations, shut-in institutions, prisons, retirement centers, offshore drilling rigs, logging camps, and remote forestry and construction camps (including transmission of the exhibition by closed circuit within the immediate area of the origin of such exhibition).
Home Video	A motion picture is released for sell-through and rental sales of packaged goods at the wholesale level, for example on DVD or Blu-Ray.
Free Television	A motion picture is released to the public on free broadcast airwaves, usually as set forth in the license agreement with networks, television stations, or basic cable networks.

Distribution Channel	Description
Pay Television	A motion picture is released to the public in a manner that requires payment by at least one participant in the broadcast chain, such as video-on-demand, cable, satellite and pay-per-view.
Internet	A motion picture is released in any one of the following online distribution channels:

Type	Description
Electronic Sell-Through (EST) or Download to Own (DTO)	Permanent digital copies sold online.
Online Rental or Video-on-Demand (VOD)	Paid rentals online for temporary viewing.
Subscription Video-on-Demand (SVOD)	Online subscription rental viewing online.
Online Free Video-on-Demand (FVOD)	Free online streaming viewing usually supported by ad revenue.
Other	Online and new media such as mobile or Internet Protocol TV.

APPENDIX C — FREQUENTLY ASKED QUESTIONS

1. **Is my service provider required to implement all of the best practices presented?**

   Compliance with best practices is strictly voluntary. They are suggested guidelines to consider when planning, implementing and modifying security procedures.

2. **Is my service provider required to apply all items included in the "Implementation Guidance" section of the best practices?**

   No. Information contained in this section of the guidelines is intended to assist you in determining the best way to structure a particular security control. If your provider has a content security assessment conducted by the MPAA, our assessment will only compare your provider's practices against the respective best practice section of the guidelines at a given point in time. (For more information about how to receive an MPAA content security assessment, you can contact us at contentsecurity@mpaa.org.)

3. **What if my current system does not allow for the implementation of best practices?**

   Please contact the respective systems vendor in order to identify possible solutions to enable systems to follow best practices. Solutions can include patching, updating the version or even changing to a more secure system. Alternative security measures can also be used if technical limitations prevent the implementation of best practices; however, these are normally not considered to cover the associated risks. Exceptions to the implementation of security guidelines due to system limitations should be formally documented and approved by your clients.

4. **When applying best practices in this guideline, will my service provider still need to comply with security requirements set individually by an MPAA Member?**

   The implementation of best practices is a guideline and does not supersede specific contractual provisions with an individual MPAA Member. Decisions regarding the use of vendor(s) by any particular Member are made by each Member solely on a unilateral basis. The MPAA encourages you to use the best practices as a guideline for future discussions around security with your clients.

APPENDIX D — REPORTING PIRACY TO THE MPAA

MPAA Report Piracy Online

You can report piracy directly to the MPAA:

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

MPAA and MPA 24-Hour Piracy Tip Lines

The following list presents the 24-hour tip line contact information for each country where the MPAA works with a local content protection office:

North America and Latin America Region	
Canada	(800) 363-9166
United States	(800) 371-9884
Europe, Middle East, Africa (EMEA) Region	
Belgium	+32 2 778 2711
Italy	(800) 864 120
Netherlands	(909) 747 2837
Ukraine	+38 0 445 013829
United Kingdom	(800) 555 111
Asia Pacific (APAC) Region	
Australia	+61 29997 8011
Hong Kong	+65 6253-1033
Malaysia	+65 6253-1033
New Zealand	+65 6253-1033
Philippines	+65 6253-1033
Singapore	+65 6253-1033
Taiwan	+65 6253-1033

A complete listing of general contact information for all content protection regional and country offices is located at: http://www.mpaa.org/contact-us/

MPAA Online Resources

Additional information about the MPAA can also be found on this website located at: www.mpaa.org

You can also learn about programs worldwide to protect content during the exhibition at: www.fightfilmtheft.org

End of Document