<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy</td>
<td>Create an information security management system that requires IT security management.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Incorporate an information security management system that requires IT security management.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Identify, implement, and assess the effectiveness of key controls to detect, analyze, and remediating security incidents.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Establish a security team that is responsible for proactively monitoring and detecting security incidents.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes third party workers.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>System/asset security and handing in general and client-specific requirements.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Disciplinary actions and management of all individuals who handle protected content.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Content/asset security and handling in general and client-specific requirements.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Inadequate or ineffective policies due to lack of control and documentation.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Establish a security team that is responsible for proactively monitoring and detecting security incidents.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes third party workers.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>System/asset security and handing in general and client-specific requirements.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Disciplinary actions and management of all individuals who handle protected content.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>System/asset security and handing in general and client-specific requirements.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
<tr>
<td></td>
<td>Inadequate or ineffective policies due to lack of control and documentation.</td>
<td>Same as above; no changes.</td>
<td>No.</td>
<td>&lt;<a href="http://www.mpaa.org/Best-practices">http://www.mpaa.org/Best-practices</a></td>
</tr>
</tbody>
</table>
Establish separate rooms for replication and mastering.

Implement fire safety measures so that in the event of a power outage, the business can continue to operate.

Disable lost electronic access devices (e.g., keycards, key fobs) in the event of a power outage.

Post security guards at all non-emergency entry/exit points.

Restrict access to production systems to authorized personnel only.

Require third party workers to be bonded and insured where required by law.

Store card stock and electronic access devices (e.g., keycards, key fobs) in locked perimeter gatehouses.

Lock perimeter gates at all times and dedicate an on-site employee to monitor and control gate access at all times.

Post security guards at all non-emergency entry/exit points.

Install door prop alarms in restricted areas (e.g., vault, server, machine room) to notify when sensitive entry/exit points are open for longer than a pre-determined period of time.

Configure alarms to provide escalation notifications directly to the appropriate security group or third party.

Maintain a detailed visitors’ log which includes the following:
- Person/people visited
- Company
- Time in/time out
- All tenants within the facility must be reported to client prior to entering other areas of the facility

Require electronic access system administration to be performed by appropriate (e.g., courier service).

Require all third party electronic access (e.g., keycards, key fobs) to be returned by the third party worker prior to being assigned to personnel.

Require international (to/from U.S.) transportation companies to be bonded and insured where required by law.

Install a centralized, audible alarm system that covers all entry/exit points.

Require access to all non-emergency entry/exit points.

Maintain a detailed visitors’ log which includes the following:
- Person/people visited
- Company
- Time in/time out
- All tenants within the facility must be reported to client prior to entering other areas of the facility

Require security requirements in third party contracts.

Perimeter Security

Entry/Exit Points

List of numbered security requirements.

Perimeter Security

Visitor Entry/Exit

Identification

Administrative Controls

Electronic Access Controls

The MPAA best practices have fundamentally changed.

The MPAA has added the requirement which qualify for Level 1 security guard, including the security protocols and investigation of incidents discovered by a security guard.

The 2015 MPAA has added the requirement which qualify for Level 1 security guard, including the security protocols and investigation of incidents discovered by a security guard.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The following table highlights the changes between the 2013 and 2015 MPAA best practices. For any new control added to the 2015 MPAA best practices, see any new highlight color. For any control which was removed from the 2015 MPAA best practices, these controls were highlighted in “grey.”

The 2015 MPAA has added one or more controls to the 2013 version.

The 2015 MPAA has generalized the use of third parties, the prior MPAA best practices had a specific focus on security audits (e.g., financial audits).

The 2015 MPAA has added the addition of safety measures in the event of a power outage. Additionally, the alarm should be deleted quarterly at a minimum.

Executive Security Awareness/Oversight
Barcode or assign unique tracking identifier(s) to client assets and use studio AKAs (“aliases”) when applicable in asset tracking systems. 

Restrict access to finished client assets to personnel responsible for their care and management.

Log and review electronic access to restricted areas for suspicious activities.

Implement additional controls to monitor security guard activity.

Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management).

Lock up and log assets that are delayed or returned if shipments could be delayed.

Store blank media/raw stock in a secured location.

Segregate duties between the vault staff and individuals who are responsible for the processing of highly sensitive content.

Maintain an ongoing log of all confirmed electronic access incidents and reconcile against surveillance footage at least daily.

Ensure that camera footage includes an accurate date and time-stamp.

PS-10.1 Implement a content asset management system to provide detailed and comprehensive tracking of client projects at all stages of the workflow process. 

PS-10.2 Log and review electronic access to restricted areas for suspicious activities.

PS-10.3 Use keys that can only be copied by a specific locksmith for exterior doors and other areas.

PS-11.2 Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in.

PS-11.3 Inventory master keys and keys to restricted areas, including facility entry/exit points, for at least 90 days, or the maximum time allowed by law, in a secure location.

PS-11.4 Designate an employee or group of employees to monitor surveillance footage at least daily.

PS-11.5 Implement a dress code policy that prohibits the use of oversized clothing (e.g., large sweaters or jackets), which could impede the ability to search individuals.

PS-12.0 Server/machine room

PS-12.1 Pre-mastering

PS-12.2 Masters/stampers vault

PS-12.3 Seat/stage/phase/colouring/immersive environments

PS-13.0 Public areas

PS-13.1 Server/machine room

PS-13.2 Pre-mastering

PS-13.3 Masters/stampers vault

PS-13.4 Seat/stage/phase/colouring/immersive environments

PS-14.0 Server/machine room

PS-14.1 Pre-mastering

PS-14.2 Masters/stampers vault

PS-14.3 Seat/stage/phase/colouring/immersive environments

PS-15.0 Establish a security presence in public areas to prevent unauthorized access to highly sensitive areas.

PS-15.1 Install a CCTV system that records all facility entry/exit points and server/machine rooms.

PS-15.2 Retain asset movement transaction logs for at least 90 days, or the maximum time allowed by law, in a secure location.

PS-15.3 Monitor the CCTV console and verify CCTV footage at least daily.

PS-15.4 Enable a camera’s ability to capture surveillance footage during operating hours and immediately investigate any identified security anomalies.

PS-15.5 Enable a camera’s ability to capture surveillance footage during operating hours and immediately investigate any identified security anomalies.

PS-15.6 Ensure that camera footage includes an accurate date and time-stamp.

PS-16.2 Perform searches upon exiting segregated areas.

PS-16.3 Performance of a self pat-down with the supervision of security personnel.

PS-16.4 Removal of all pocket contents.

PS-16.5 Randomly search persons, bags, packages, and personal items for client assets.

PS-17.0 Black Media/Year Book Tracking

PS-17.1 Use studio film title aliases when applicable on physical assets and in all systems.

PS-17.2 Use keys that can only be copied by a specific locksmith for exterior doors and other areas.

PS-18.0 Black Media/Year Book Tracking

PS-18.1 Log and review electronic access to restricted areas for suspicious activities.

PS-18.2 Implement a content asset management system to provide detailed and comprehensive tracking of client projects at all stages of the workflow process.

PS-18.3 Log and review electronic access to restricted areas for suspicious activities.

PS-18.4 Use keys that can only be copied by a specific locksmith for exterior doors and other areas.

PS-18.5 Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management).

PS-18.6 Lock up and log assets that are delayed or returned if shipments could be delayed.

PS-18.7 Store blank media/raw stock in a secured location.

PS-18.8 Segregate duties between the vault staff and individuals who are responsible for the processing of highly sensitive content.

PS-18.9 Maintain an ongoing log of all confirmed electronic access incidents and reconcile against surveillance footage at least daily.

PS-18.10 Ensure that camera footage includes an accurate date and time-stamp.

PS-19.0 Install a CCTV system that records all facility entry/exit points and server/machine rooms.

PS-19.1 Retain asset movement transaction logs for at least 90 days, or the maximum time allowed by law, in a secure location.

PS-19.2 Monitor the CCTV console and verify CCTV footage at least daily.

PS-19.3 Enable a camera’s ability to capture surveillance footage during operating hours and immediately investigate any identified security anomalies.

PS-19.4 Ensure that camera footage includes an accurate date and time-stamp.

PS-20.0 Log and review electronic access to restricted areas for suspicious activities.

PS-20.1 Implement a content asset management system to provide detailed and comprehensive tracking of client projects at all stages of the workflow process.

PS-20.2 Log and review electronic access to restricted areas for suspicious activities.

PS-20.3 Use keys that can only be copied by a specific locksmith for exterior doors and other areas.

PS-20.4 Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management).

PS-20.5 Lock up and log assets that are delayed or returned if shipments could be delayed.

PS-20.6 Store blank media/raw stock in a secured location.

PS-20.7 Segregate duties between the vault staff and individuals who are responsible for the processing of highly sensitive content.

PS-20.8 Maintain an ongoing log of all confirmed electronic access incidents and reconcile against surveillance footage at least daily.

PS-20.9 Ensure that camera footage includes an accurate date and time-stamp.

PS-21.0 Log and review electronic access to restricted areas for suspicious activities.

PS-21.1 Implement a content asset management system to provide detailed and comprehensive tracking of client projects at all stages of the workflow process.

PS-21.2 Log and review electronic access to restricted areas for suspicious activities.

PS-21.3 Use keys that can only be copied by a specific locksmith for exterior doors and other areas.

PS-21.4 Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management).

PS-21.5 Lock up and log assets that are delayed or returned if shipments could be delayed.

PS-21.6 Store blank media/raw stock in a secured location.

PS-21.7 Segregate duties between the vault staff and individuals who are responsible for the processing of highly sensitive content.

PS-21.8 Maintain an ongoing log of all confirmed electronic access incidents and reconcile against surveillance footage at least daily.

PS-21.9 Ensure that camera footage includes an accurate date and time-stamp.

PS-22.0 Log and review electronic access to restricted areas for suspicious activities.

PS-22.1 Implement a content asset management system to provide detailed and comprehensive tracking of client projects at all stages of the workflow process.

PS-22.2 Log and review electronic access to restricted areas for suspicious activities.

PS-22.3 Use keys that can only be copied by a specific locksmith for exterior doors and other areas.

PS-22.4 Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management).

PS-22.5 Lock up and log assets that are delayed or returned if shipments could be delayed.

PS-22.6 Store blank media/raw stock in a secured location.

PS-22.7 Segregate duties between the vault staff and individuals who are responsible for the processing of highly sensitive content.

PS-22.8 Maintain an ongoing log of all confirmed electronic access incidents and reconcile against surveillance footage at least daily.

PS-22.9 Ensure that camera footage includes an accurate date and time-stamp.
<table>
<thead>
<tr>
<th>Control Set</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS-1.0</td>
<td>Implement a dedicated, secure area (e.g., security cage, secure room for receiving and unloading of shipments).</td>
</tr>
<tr>
<td>DS-1.3</td>
<td>Lock automobiles and trucks at all times, and do not place packages in a driver’s cab or sleeper berth.</td>
</tr>
<tr>
<td>DS-1.5</td>
<td>Place externally accessible servers (e.g., web servers) within the DMZ.</td>
</tr>
<tr>
<td>PS-17.0</td>
<td>Require personnel picking up package(s) to verify the count of the items, and correlate it to the count on the waybill.</td>
</tr>
<tr>
<td>PS-17.1</td>
<td>Tamper-evident seals (e.g., in the form of holograms) should be used to ensure the security of client assets.</td>
</tr>
<tr>
<td>PS-17.5</td>
<td>Assign a tracking number for each shipment as it leaves the facility.</td>
</tr>
<tr>
<td>PS-18.0</td>
<td>Observe and monitor the on-site packing and sealing of trailers prior to delivery.</td>
</tr>
<tr>
<td>PS-18.1</td>
<td>Require that rejected, damaged, and obsolete stock containing sensitive or restricted information be destroyed as soon as possible, and stored with surveillance cameras and/or security guards.</td>
</tr>
<tr>
<td>PS-18.2</td>
<td>Do not allow remote access to WAN network infrastructure devices (e.g., firewalls, routers) that control access to content unless at least two authorized individuals are physically present, and can verify the identity and authorization of each individual.</td>
</tr>
</tbody>
</table>

**Shipping**

- **DS-1.0** Implement a formal process to record, monitor, and review travel times, tracking information, and receipt of deliveries.
- **PS-17.0** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-17.1** Tamper-evident seals (e.g., in the form of holograms) should be used to ensure the security of client assets.
- **PS-17.2** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.0** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.1** Require that rejected, damaged, and obsolete stock containing sensitive or restricted information be destroyed as soon as possible, and stored with surveillance cameras and/or security guards.

**Handling**

- **PS-17.0** Implement a formal process to record, monitor, and review travel times, tracking information, and receipt of deliveries.
- **PS-17.1** Tamper-evident seals (e.g., in the form of holograms) should be used to ensure the security of client assets.
- **PS-17.2** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.0** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.1** Require that rejected, damaged, and obsolete stock containing sensitive or restricted information be destroyed as soon as possible, and stored with surveillance cameras and/or security guards.
- **PS-18.2** Do not allow remote access to WAN network infrastructure devices (e.g., firewalls, routers) that control access to content unless at least two authorized individuals are physically present, and can verify the identity and authorization of each individual.

**Packing**

- **PS-17.0** Implement a formal process to record, monitor, and review travel times, tracking information, and receipt of deliveries.
- **PS-17.1** Tamper-evident seals (e.g., in the form of holograms) should be used to ensure the security of client assets.
- **PS-17.2** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.0** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.1** Require that rejected, damaged, and obsolete stock containing sensitive or restricted information be destroyed as soon as possible, and stored with surveillance cameras and/or security guards.
- **PS-18.2** Do not allow remote access to WAN network infrastructure devices (e.g., firewalls, routers) that control access to content unless at least two authorized individuals are physically present, and can verify the identity and authorization of each individual.

**Forward/Returns/Reclamation Facility**

- **PS-17.0** Implement a formal process to record, monitor, and review travel times, tracking information, and receipt of deliveries.
- **PS-17.1** Tamper-evident seals (e.g., in the form of holograms) should be used to ensure the security of client assets.
- **PS-17.2** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.0** Observe and monitor the on-site packing and sealing of trailers prior to delivery.
- **PS-18.1** Require that rejected, damaged, and obsolete stock containing sensitive or restricted information be destroyed as soon as possible, and stored with surveillance cameras and/or security guards.
- **PS-18.2** Do not allow remote access to WAN network infrastructure devices (e.g., firewalls, routers) that control access to content unless at least two authorized individuals are physically present, and can verify the identity and authorization of each individual.
Establish and implement an account management process for I/O devices. Only approved users shall have software installation privileges.

Install anti-virus software on all workstations, servers, and laptops. At least once per week, perform virus scans on systems used for content handling or storage.

Restrict remote access to the content/production network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Establish and implement logical network segmentation. LAN/WAN/Internet networks shall be segregated to the extent that is technologically feasible.

Secure backups of local area network (SAN/NAS), devices, servers and workstations to be centrally secured on all the internal LAN.

Restrict access to systems that process or store digital content, only to approved personnel.

Enable full system virus and malware scans for servers, where applicable (e.g., non-production network servers, such as I/O server networks). Systems used for content storage on SAN/NAS systems must have virus scans enabled.

Restrict the use of non-switched devices (e.g., hubs and repeaters) on the content/production network. Disable all unused switch ports on the content/production network.

Secure any point to point connections by using dedicated, private connections and by using encryption.

Perform quarterly vulnerability scans of all external IP ranges and hosts to assess security posture and to determine the need for updated or additional security measures.

Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.

Restrict access to the content/production systems to authorized users.

Restrict access to the content/production systems to authorized users.

Prohibit users from being Administrators on their own workstations, laptops, workstations, servers) that are set up internally.

Protect laptops, tablets, cloud computing devices (e.g., MacBook, etc.) in all systems that handle or store content, with the exception of systems used for content handling or outputting I/O devices to physical media.

Prohibit dual-homed networking (physical networked bridging) on any systems that handle or store or process or transfer digital content.

Perform scans as follows:

Systems Security

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Restrict access to systems that process or store digital content, only to approved personnel.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.

Limit the implementation of access to the third-party network to only those who are necessary to perform work. Additional restriction processes and protocols shall be implemented.
Account Management

- Enable logging of internal and external content movement and transfers.
- Review logs weekly.
- Implement two-factor authentication (e.g., username/password and out-of-band communication).
- Send decryption keys or passwords using an out-of-band communication channel.
- Rename the default administrator accounts and other default accounts.
- Establish a process for key management that addresses the following:
  - Key generation
  - Key distribution
  - Key management
  - Key revocation

Executive Security Awareness/Oversight

- Enforce a strong password policy for gaining access to information systems.
- Rename the default administrator accounts and limit the use of these credentials (e.g., operating system updates, patch installations).
- Send decryption keys or passwords using an out-of-band communication channel.
- Ensure that security techniques (e.g., spoiling, invisible/visible watermarks) are available for use and are applied consistently.
- Develop a BYOD (Bring Your Own Device) policy for mobile devices.
- Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.
- Investigate any unusual activity reported by the logging and reporting systems.
- Provide a layered authentication strategy for WAN and LAN/remote access to information systems.

Authentication

- Establish a policy for secure communication and passwords to access information systems.
- Establish a strong password policy for gaining access to information systems.
- Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.
- Implement password-protected screensavers or screen-lock software for all systems and mobile devices.
- Provide improved additional authentication mechanisms for all information systems.
- Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum:
  - What (content)
  - Where (location)
  - When (timestamp)
  - How (activity)
  - By whom (account)

Logging and Monitoring

- Review all logs weekly, and review all critical and high events.
- Audit logging of internal and external content movement and transfers and provide a logs file at a minimum:
  - Who (account)
  - What (content)
  - When (timestamp)
  - Where (location)
  - Why (activity)

Mobile Security

- Establish a STRIDE (Spoofing, Repudiation, Denial of Service, Information Theft, Remote Access, Elevation of Privilege) policy for mobile devices.
- Establish a KSA (KSA: Access, Application, and Information) policy for mobile devices.
- Implement log collection of mobile devices as outlined in the Mobile Security section of the 2015 MPAA best practices.
- Implement log collection of mobile devices as outlined in the Mobile Security section of the 2015 MPAA best practices.
- Implement automatic logging of the device after 30 minutes of inactivity.
- Manage all mobile device operating system patches and application updates.
- Establish password policies.
- Implement a system for password backup and maintenance of mobile devices.

Security Techniques

- Implement key management policies and procedures to ensure the recognition of content or code, regardless of its location (e.g., servers, databases, workstations, firewalls, mobile devices, local, email).
- Approve and issue encryption of content keys.
- Implement a standard to monitor and control distribution of content keys.
- Develop a policy to support management of encryption keys.
- Develop a policy to support management of encryption keys.
- Establish a policy to support key management.
- Establish a policy to support key management.
- Implement key management procedures and key backup procedures.
<table>
<thead>
<tr>
<th>Security Topic</th>
<th>MPAA Best Practices 2013</th>
<th>Additions to the differences between 2013 and 2015 version</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS-13.5</td>
<td>Review access to the client web portal at least quarterly</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.6</td>
<td>Implement a digital content management system to provide detailed tracking of digital content.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.7</td>
<td>Implement transfer tools that use access controls, where clients request and to authorize clients, produce exceptions to the production protocol.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.8</td>
<td>Monitor access to the content/production network, where content is stored, and for suspicious activities.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.9</td>
<td>Implement an exception policy, where clients' prior approval must be obtained in writing, to address situations where encrypted transfer tools are used.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.10</td>
<td>Establish access to web portals which are valid for transferring content, containing content and key distribution to authorized users.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.11</td>
<td>Design unique credentials (e.g., username and password) for portal users and distribute credentials to clients securely.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.12</td>
<td>Implement web portal access controls within the DMZ and limit access to/from specific IPs and protocols.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.13</td>
<td>Protect the use of the content production software/systems/complexes that are hosted on an internet web server unless approved by the client in advance.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.14</td>
<td>Enforce use of a strong cipher suite (e.g., TLSv1.2) for the internal/external web portal.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.15</td>
<td>Implement automatic monitoring and distribute credentials to clients securely.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.16</td>
<td>Protect the content/production network, where content is stored, and for suspicious activities.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.17</td>
<td>Monitor access to the content/production network, where content is stored, and for suspicious activities.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.18</td>
<td>Implement web content security protocols, to be reviewed at least annually vs. periodically.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.19</td>
<td>Implement an exception policy, where clients' prior approval must be obtained in writing, to address situations where encrypted transfer tools are used.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.20</td>
<td>Establish access to web portals which are valid for transferring content, containing content and key distribution to authorized users.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.21</td>
<td>Design unique credentials (e.g., username and password) for portal users and distribute credentials to clients securely.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.22</td>
<td>Implement web portal access controls within the DMZ and limit access to/from specific IPs and protocols.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.23</td>
<td>Protect the use of the content production software/systems/complexes that are hosted on an internet web server unless approved by the client in advance.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.24</td>
<td>Enforce use of a strong cipher suite (e.g., TLSv1.2) for the internal/external web portal.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.25</td>
<td>Implement automatic monitoring and distribute credentials to clients securely.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.26</td>
<td>Protect the content/production network, where content is stored, and for suspicious activities.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.27</td>
<td>Monitor access to the content/production network, where content is stored, and for suspicious activities.</td>
<td>2015 MPAA added this control.</td>
</tr>
<tr>
<td>DS-13.28</td>
<td>Implement an exception policy, where clients' prior approval must be obtained in writing, to address situations where encrypted transfer tools are used.</td>
<td>2015 MPAA added this control.</td>
</tr>
</tbody>
</table>

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices reference: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the differences between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.

- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "Blue.
- For any control which was removed from the 2015 MPAA best practices, these controls were highlighted in "Green."