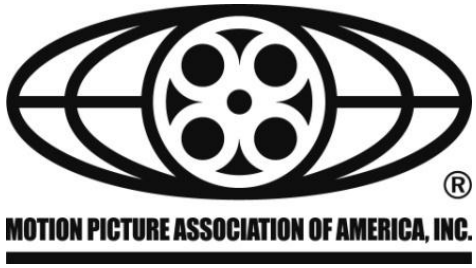


**MPAA Site Security Program**

# CONTENT SECURITY BEST PRACTICES

# REPLICATION SUPPLEMENTAL

Version 2.0

May 15, 2011

# DOCUMENT HISTORY

| Version | Date | Description | Author |
|---|---|---|---|
| 1.0 | December 31, 2009 | Initial Public Release | Deloitte & Touche LLP<br>MPAA<br>MPAA Member Companies |
| 2.0 | May 15, 2011 | Updates and Revisions<br>Consolidation into Common Guidelines and Supplementals | PwC LLP<br>MPAA<br>MPAA Member Companies |

# I. Replication Overview

## General Description

Replication facilities are responsible for the mass production of DVDs to be distributed to the home entertainment market. These facilities handle large volumes of finished consumer goods that are packaged and ready for distribution.

## Facility

The following table describes the attributes of the content generally held at this facility type:

**Type of Content**

☐ Stills
☐ Script
☐ Audio Only
☑ Video and Audio

| Video Attribute | Description |
|---|---|
| Completeness | ☑ Full<br>☐ Partial |
| Resolution | ☑ High<br>☐ Low |
| Quality | ☑ Clean<br>☐ Watermarked<br>☐ Spoiled |

## Typical Risks

Typical security and content protection risks for this facility type include, but are not limited to, the following:

- Loss, interception or theft of sensitive content such as:
  - Finished consumer goods
  - DVD masters
  - Stampers
- Large volume of physical content awaiting fulfillment
- Small size of consumer goods that makes theft easier
- Lack of security awareness around content loss and theft
- Ad-hoc processes around the following areas:
  - Destruction of scrap DVDs and rejects
  - Notification of losses and theft of missing content
  - Asset classification and education on handling highly sensitive content
  - Shipping and receiving counts
- Dangerous facility locations

# II. BEST PRACTICE SUPPLEMENTAL GUIDELINES

| MANAGEMENT SYSTEM | | PHYSICAL SECURITY | | | DIGITAL SECURITY | | |
|---|---|---|---|---|---|---|---|
| ORGANIZATION AND MANAGEMENT | COMPETENCY | FACILITY | ASSET MANAGEMENT | TRANSPORT | INFRASTRUCTURE | CONTENT MANAGEMENT | CONTENT TRANSFER |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| MS.S-1.0 | Executive Security Awareness / Oversight | Establish an information security management system that implements a control framework (e.g., IS0 27001) for information security which is approved by executive management / owner(s) | |
| MS.S-3.0 | Security Organization | Establish a security team that is responsible for proactively monitoring **information systems** and physical security to identify and respond to any suspicious activity | • Monitor **information systems** regularly throughout the day to detect possible incidents<br>• Incorporate the **incident response** process to handle detected incidents<br>• Consider implementing automatic notification to the team when suspicious activity involving **information systems** is detected<br>• Implement a periodic review process to monitor the effectiveness of monitoring processes |

| MANAGEMENT SYSTEM | | PHYSICAL SECURITY | | | DIGITAL SECURITY | | |
|---|---|---|---|---|---|---|---|
| ORGANIZATION AND MANAGEMENT | COMPETENCY | FACILITY | ASSET MANAGEMENT | TRANSPORT | INFRASTRUCTURE | CONTENT MANAGEMENT | CONTENT TRANSFER |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| MS.S-11.0 | Disciplinary Measures | Include a provision in the disciplinary policy stating that a lack of cooperation with the exit search procedure can lead to disciplinary actions | • Identify appropriate disciplinary measures that are aligned with the severity and business impact of any security-related breaches caused by the individual<br>• Involve senior management in determining the actions to be applied<br>• Communicate potential sanctions to all **company personnel** and **third party workers**<br>• Document the measures in the company handbook, security policies and other areas<br>• Communicate disciplinary measures in new hire orientation training |
| MS.S-12.0 | Content Security and Piracy Awareness | Provide in-depth training specific to the content handled by the facility | • Include security training on risks surrounding the transport and handling of content<br>• Emphasize the individual responsibilities of each job function to protect content and mitigate piracy issues<br>• Integrate training material to include the MPAA "Report Piracy" website and studio/client contact information<br>• Provide internal anonymous telephone number and/or website to report piracy |
| MS.S-13.0 | Third Party Use and Screening | Communicate to clients the use of third-party storage providers for physical assets | • Provide clients with **due diligence** reports for third party storage companies<br>• Require clients to approve and sign-off on the use of third party storage companies |
| MS.S-13.1 | | Require international (to/from U.S.) transportation companies to be "Customs-Trade Partnership Against Terrorism" (CTPAT) certified | • Require international transportation companies to present proof of CTPAT certification upon first hire<br>• Maintain a list of CTPAT certified transportation companies |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| MS.S-13.2 | | Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services | • Implement procedures to track which vendors have undergone **due diligence** for the year (e.g., database repository, certificates of completion) |
| MS.S-13.4 | | Incorporate security **due diligence** activities (e.g., security assessment, self-assessment questionnaire) as part of a selection and hiring process for **third party workers** who handle sensitive content | • Consider the following:<br>– Require **third party workers** to provide their policies and procedures for handling content<br>– Conduct interviews with the third party's management and key process owners to identify content handling procedures / controls for processing, storing and transmitting sensitive content<br>– Request the third party to provide security **risk assessment** results and relevant remediation plans |

| MANAGEMENT SYSTEM | | PHYSICAL SECURITY | | | DIGITAL SECURITY | | |
|---|---|---|---|---|---|---|---|
| ORGANIZATION AND MANAGEMENT | COMPETENCY | FACILITY | ASSET MANAGEMENT | TRANSPORT | INFRASTRUCTURE | CONTENT MANAGEMENT | CONTENT TRANSFER |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-1.0 | Entry/Exit Points | Post security guards at all non-emergency entry/exit points | • Require security guards to visually inspect all individuals leaving the facility<br>• Implement a process by which guards report and investigate suspicious behavior |
| PS.S-1.1 | | Lock and install alarms on all loading dock doors, and monitor loading dock doors while in use | • Unlock loading docks only for transactions that have a valid work order<br>• Require the appropriate **company personnel** to be present at all times during loading |
| PS.S-1.2 | | Segregate the truck driver's entrance to prevent truck drivers from entering other areas of the facility | |
| PS.S-1.3 | | Implement a daily security patrol process with a randomized schedule and document patrolling results in a log | • Require security guards to patrol both interior and exterior areas<br>• Include a review of emergency exits, including verification of seals<br>• Consider using a guard tour patrol system to track patrolling (e.g., Checkpoint) and verify locks |
| PS.S-1.4 | | Document, investigate, and resolve all incidents detected during security guard shifts | • Establish guidelines for triggering the **incident response** process<br>• Incorporate **incident response** procedures for handling detected security events |
| PS.S-4.0 | Perimeter Security | Install additional perimeter safeguards (e.g., fences, vehicle barricades) to decrease the risk of unauthorized access onto the premises | • Install fences that are high enough to mitigate unauthorized entry<br>• Position vehicle barricades to reduce the likelihood of forced vehicular entry |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-4.1 | | Lock perimeter gates at all times and dedicate an on-site employee to handle remote unlocking capabilities | • Assign the front desk personnel the responsibility of managing visitor requests for entry<br>• Place cameras at perimeter gates to verify visitor identity |
| PS.S-4.2 | | Station a security guard at perimeter entrances and implement a process (e.g., electronic gate arm, parking permits) to allow vehicles into the facility campus | • Implement an electronic arm, that is manned by security personnel, to control vehicle access into the facility<br>• Distribute parking permits to **company personnel** and **third party workers** who have completed proper paperwork<br>• Require visitor vehicles to present identification and ensure that all visitors have been pre-authorized to enter the premises |
| PS.S-5.0 | Emergency Protocol | Establish and enforce emergency congregation areas and account for all personnel after evacuating the facility | • Prohibit individuals from going to their vehicles and lockers and from leaving emergency congregation areas |
| PS.S-7.0 | Authorization | Review access to restricted areas (e.g., **vault**, safe) on a monthly basis and when the roles or employment status of any **company personnel** and/or **third party workers** change | • Validate the status of **company personnel** and **third party workers**<br>• Verify that access remains appropriate for each users' associated job function |
| PS.S-10.0 | Cameras | Review camera positioning, image quality, frame rate and retention daily | • Review camera positioning to ensure full coverage of all entry/exit points and other sensitive areas<br>• Review image quality to ensure that lighting is adequate and that faces are distinguishable<br>• Review surveillance logs to ensure that logs are being retained for at least 90 days |
| PS.S-10.1 | | Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents | • Incorporate the **incident response** process for handling detected security incidents |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-11.0 | Logging and Monitoring | Perform a weekly review of electronic access logs for the following areas, if applicable:<br>• Masters/stampers **vault**<br>• Pre-mastering<br>• Server/machine room<br>• Scrap room<br>• High-security cages | • Identify and document events that are considered unusual<br>• Consider the implementation of an automated reporting process that sends real-time alerts to the appropriate security personnel when suspicious electronic access activity is detected |
| PS.S-12.0 | Searches | Implement an exit search process that is applicable to all facility personnel and visitors, including:<br>• Removal of all outer coats, hats, and belts for inspection<br>• Removal of all pocket contents<br>• Performance of a self pat-down with the supervision of security<br>• Thorough inspection of all bags<br>• Inspection of laptops' CD/DVD tray<br>• Scanning of individuals with a handheld metal detector used within three inches of individual searched | • Instruct security guards to look for items that are restricted from being brought onsite (e.g., cameras) or film materials which are not allowed to be brought offsite without proper authorization<br>• Communicate policies regarding exit search to all **company personnel** and **third party workers**<br>• Stagger shift changes to prevent long lines and extended wait times |
| PS.S-12.1 | | Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., **USB** thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure | • Confiscate any digital recording devices that are detected and store them in secured lockers<br>• Document any incidents of attempted content theft<br>• Take the necessary disciplinary action for individuals attempting content theft<br>• Implement and enforce a policy to prohibit mobile / cellular devices with digital recording capabilities.<br>• Allow cell phones with digital recording capabilities if tamper-evident stickers are used |
| PS.S-12.2 | | Enforce the use of transparent plastic bags and food containers for any food brought into production areas | • Consider designating an area for eating food outside of the production area |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-12.3 | | Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts) | |
| PS.S-12.4 | | Use numbered, tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility | |
| PS.S-12.5 | | Implement a process to test the exit search procedure | • Perform periodic audits of the search process to ensure that security guards are thorough with their searches<br>• Identify ways to improve the exit search process<br>• Document all audits of and improvements to the search process |
| PS.S-12.6 | | Perform a random vehicle search process when exiting the facility parking lot | |
| PS.S-12.7 | | Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas | |
| PS.S-12.8 | | Implement additional controls to monitor security guard activity | • Review exit search process for security guards upon exit<br>• Segregate security guards that oversee plant/production with exit points (e.g., search process) |

| MANAGEMENT SYSTEM | | PHYSICAL SECURITY | | | DIGITAL SECURITY | | |
|---|---|---|---|---|---|---|---|
| ORGANIZATION AND MANAGEMENT | COMPETENCY | FACILITY | ASSET MANAGEMENT | TRANSPORT | INFRASTRUCTURE | CONTENT MANAGEMENT | CONTENT TRANSFER |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-13.0 | Inventory Tracking | Use automated notification for assets that have been out of the **vault** for extended periods of time | • Establish expected check-out durations for each type of asset<br>• Configure the content asset management system to automatically notify **vault** personnel when assets have not been returned within the expected timeframe |
| PS.S-14.0 | Inventory Counts | Perform a weekly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients | • Document all inventory counts<br>• Do not allow **vault** staff to perform inventory counts (i.e., **segregation of duties**) |
| PS.S-15.0 | Blank Media/ Raw Stock Tracking | Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly | • Reconcile existing raw stock with work orders to identify variances in inventory<br>• Establish a variance threshold that triggers the **incident response** process when exceeded<br>• Consider the execution of physical counts of raw stock as part of the monthly tracking process |
| PS.S-16.0 | Client Assets | Require two **company personnel** with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours | |
| PS.S-16.1 | | Use an access-controlled cage for the **staging area** and always monitor the area with surveillance cameras | |
| PS.S-18.0 | Disposals | Implement a process that requires security personnel to monitor and record the scrapping process if scrap is destroyed | • Ensure that scrapped assets are unusable and cannot be copied<br>• Maintain records of all scrap that is destroyed |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-18.1 | | Conduct periodic security training for all **company personnel** and **third party workers** to educate on asset disposal and destruction processes (e.g., placing assets into designated containers) | • Require **company personnel** and **third party workers** to receive asset disposal and destruction training as it pertains to their job functions<br>• Implement procedures to track which individuals have undergone training for the year (e.g., database repository, certificates of completion) |
| PS.S-18.2 | | Scratch discs before placing them into the scrap bin | • Consider shredding the medium prior to going into the scrap bin |
| PS.S-18.3 | | Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling) | • Use **segregation of duties** (e.g., personnel who create the check disc is separate from personnel who destroy the disc) where automated disposal is not an option<br>• Maintain a signed log of the date and time, on which the disc was disposed |

| MANAGEMENT SYSTEM | | PHYSICAL SECURITY | | | DIGITAL SECURITY | | |
|---|---|---|---|---|---|---|---|
| ORGANIZATION AND MANAGEMENT | COMPETENCY | FACILITY | ASSET MANAGEMENT | TRANSPORT | INFRASTRUCTURE | CONTENT MANAGEMENT | CONTENT TRANSFER |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-19.0 | Shipping | Document and retain a separate log for truck driver information | • Maintain a log of all truck drivers and include the following information:<br>– Name<br>– License tags for the tractor and trailer<br>– Affiliated company<br>– Time and date of pick up<br>– Content handled |
| PS.S-19.1 | | Require personnel picking up package(s) to verify the count against shipping document and obtain a signature from the shipping point | • Require recipients to reconcile that the shipped count matches their work orders<br>• Report back any discrepancies or damage to shipped goods immediately |
| PS.S-19.2 | | Observe and monitor the packing and sealing of trailers when shipping occurs on-site | • Require security personnel to be present at all times while trailers are loaded and sealed |
| PS.S-19.3 | | Implement a formal process to record, monitor, and review travel times, routes, and delivery times for shipments between facilities | • Establish a baseline for delivery times between common shipping points and monitor actual times for variance<br>• Investigate, report, and escalate major variances to appropriate personnel<br>• Designate approved rest stops |
| PS.S-22.0 | Packaging | Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped | • Apply shrink wrapping to individual assets (e.g., skids, pallets) or per spindle if bulk shipments are performed |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| PS.S-23.0 | Transport Vehicles | Include the following security features in transportation vehicles (e.g., trailers):<br>• Segregation from driver cabin<br>• Ability to lock and seal cargo area doors<br>• GPS for high-security shipments | • Use vehicles equipped with GPS or XDA tracking systems for delivery of sensitive content and high-value assets |
| PS.S-23.1 | | Apply numbered seals on cargo doors for shipments of highly sensitive titles | • Require security guards to apply, record, and monitor seals<br>• Consider additional security measures for highly sensitive packages (e.g., locked/secured cargo area, locked pelican cases) |
| PS.S-23.2 | | Require security escorts be used for delivery of highly sensitive content in high-risk areas | • Hire security personnel capable of protecting highly sensitive content from hijacking, mugging, and other scenarios which could result in content theft |

| MANAGEMENT SYSTEM | | PHYSICAL SECURITY | | | DIGITAL SECURITY | | |
|---|---|---|---|---|---|---|---|
| ORGANIZATION AND MANAGEMENT | COMPETENCY | FACILITY | ASSET MANAGEMENT | TRANSPORT | INFRASTRUCTURE | CONTENT MANAGEMENT | CONTENT TRANSFER |

| No. | Security Topic | Best Practice | Implementation Guidance |
|---|---|---|---|
| N/A | Digital Security | This facility service does not generally have digital content. **Consequently, none of the digital controls in the *Common Guidelines* apply.** | |

# APPENDIX A — MAPPING OF SUPPLEMENTAL CONTROLS TO REFERENCES

The following table provides a general mapping of the best practices to the ISO 27001/27002 and NIST 800-53 standards. These standards can be referenced for further information on the implementation of the provided security controls.

| No. | Security Topic | ISO 27002 Reference | NIST Reference |
|---|---|---|---|
| **MS.S-1.0** | Executive Security Awareness / Oversight | 6.1.1, 6.1.2 | PM-1, PM-2 |
| **MS.S-3.0** | Security Organization | 6.1.3 | PE-6, PM-2, SI-4 |
| **MS.S-11.0** | Disciplinary Measures | 5.1.1, 8.2.2, 8.2.3 | AT-2, PS-8 |
| **MS.S-12.0** | Content Security and Piracy Awareness | 8.2.2 | AT-3, CP-3 |
| **MS.S-13.0** | Third Party Use and Screening | 6.2.1 | |
| **MS.S-13.2** | | 6.2.3, 10.2.2 | PS-3 |
| **MS.S-13.4** | | 6.2.3, 8.1.2, 10.2 | PS-3 |
| **PS.S-1.1** | | 9.1.6 | PE-3, PE-7, PE-16 |
| **PS.S-1.2** | | 9.1.2, 9.1.6 | PE-3 , PE-7, PE-16 |
| **PS.S-1.3** | | | PE-1 |
| **PS.S-1.4** | | 13.1.1, 13.1.2 | IR-1 |
| **PS.S-4.0** | Perimeter | 9.1.1 | PE-3 |

| No. | Security Topic | ISO 27002 Reference | NIST Reference |
|---|---|---|---|
| **PS.S-4.1** | Security | 9.1.1 | PE-3 |
| **PS.S-4.2** | | 9.1.1 | PE-3 |
| **PS.S-5.0** | Emergency Protocol | 14.1.4 | |
| **PS.S-7.0** | Authorization | 9.1.2, 11.2.4 | PE-2, PE-3, PE-6 |
| **PS.S-10.0** | Cameras | 9.1.1 | PE-3, PE-6 |
| **PS.S-10.1** | | 6.1.3, 9.1.1 | IR-5, IR-6, PE-3, PE-6 |
| **PS.S-11.0** | Logging and Monitoring | 9.1.2, 10.10 | PE-6 |
| **PS.S-12.1** | | 7.1.3, 9.1.5, 9.2.7 | AC-19 |
| **PS.S-12.4** | | | MP-3 |
| **PS.S-12.8** | | 10.1.3 | AC-5 |
| **PS.S-13.0** | Inventory Tracking | | SI-5 |
| **PS.S-14.0** | Inventory Counts | 7.1.1 | CM-8 |
| **PS.S-16.0** | Client Assets | 10.1.3 | AC-5 |
| **PS.S-16.1** | | 9.1.2 | PE-3, PE-6 |
| **PS.S-18.1** | | 8.2.2, 9.2.6, 10.7.2 | AT-2, AT-3, MP-6 |

| No. | Security Topic | ISO 27002 Reference | NIST Reference |
|---|---|---|---|
| **PS.S-18.2** | | 9.2.6 | MP-6 |
| **PS.S-19.0** | Shipping | 10.8.2, 10.8.3 | MP-5, SA-9 |
| **PS.S-19.1** | | 10.8.2, 10.8.3 | |
| **PS.S-19.2** | | 10.8.3 | MP-5, PE-16 |
| **PS.S-19.3** | | 10.8.2 | MP-5, PE-16 |
| **PS.S-22.0** | Packaging | 10.8.3 | |
| **PS.S-23.1** | | 10.8.3 | |

**End of Document**