



Content Delivery and Storage Association

Anti-Piracy and Compliance Programs

APCP: Content Protection and Security Standards and Procedures, version 3.0

01 June 2008, Copyright © 2008 Content Delivery & Storage Association

Introduction

The Content Delivery & Storage Association (CDSA) *APCP: Content Protection and Security Standards & Procedures* is part of the CDSA Anti-Piracy and Compliance Programs (APCP), an industry-driven initiative designed to protect intellectual property – electronic and physical products - in the supply chain. These Standards and Procedures apply to, but are not limited to, supply chain points from content creation, production, digital compression, encoding and authoring to manufacturing and distribution of final product. These CDSA *APCP: Content Protection and Security Standards and Procedures* have been developed by a task force representing intellectual property owners and their manufacturers and suppliers along the content delivery supply chain.

The objective of these CDSA *APCP: Content Protection and Security Standards and Procedures* is to provide supply chain partners of client content owners a framework for managing and safeguarding intellectual property, analog and digital assets, and physical products in a secure manner, and minimizing risks to an acceptable level by:

- implementing processes to organize, inventory, track and manage clients' assets,
- preventing unauthorized access, disclosure and/or alteration of clients' assets,
- preventing loss of income and content assets through theft, loss, damage, misuse or other exploitation of clients' assets,
- addressing any identified security control weakness or failing within the certified site, and
- mitigating or preventing loss of assets or asset integrity upon the cessation of the business relationship between the client and certified site.

Other aspects of piracy prevention and good business practices, such as protecting intellectual property by adhering to copyright laws and processes, are addressed in other Standards and Procedures within the CDSA Anti-Piracy and Compliance Programs.

These CDSA *APCP: Content Protection and Security Standards and Procedures* specify minimum system security requirements for protection of client assets and products by sites providing services to intellectual property owner clients or their agents, including, but not limited to the:

- creative production of content,
- compression, encoding and/or authoring of content,
- manufacture, assembly, storage, transmission and/or delivery of key components and finished intellectual property products.

Sections 1 through 4 of these CDSA *APCP: Content Protection and Security Standards and Procedures* describe the minimum internal procedures and requirements that must be in place for a site to be in compliance with the CDSA *APCP: Content Protection and Security Standards & Procedures*. They represent the essence of good business practices and are aligned with the requirements of ISO 9001:2000 and ISO 17799:2005 (ISO/IEC 27002:2005) standards.

Sections 5 though 7 describe specific technical requirements tailored specifically to content creation, production, management, control, manufacturing, packaging and delivery processes for asset security that must be also in place in order for a site to be in compliance with the CDSA *APCP: Content Protection and Security Standards & Procedures*.

1. PERSONNEL AND RESOURCES

- 1.1. The CDSA *APCP: Content Protection and Security Standards and Procedures* are designed to protect intellectual property, analog and digital assets, and physical products in the supply chain. This purpose must be understood and maintained throughout the organization at the site.
- 1.2. Site management shall prepare a security policy that:
 - 1.2.a. is appropriate to the site's organization and its processes,
 - 1.2.b. demonstrates a commitment to meeting asset security requirements,
 - 1.2.c. demonstrates a commitment to continuous improvement of the security systems,
 - 1.2.d. is communicated and understood by personnel within the site's organization, and
 - 1.2.e. is reviewed periodically to ensure its continuing suitability.
- 1.3. The responsibility and authority of personnel involved with content protection and security work shall be defined in writing and shall include at a minimum their authority to:
 - 1.3.a. identify and provide resources to establish, implement, maintain and control content protection and security system policies and procedures,
 - 1.3.b. appoint a security management system program manager who shall ensure that the security management system and its policies and procedures are established,

implemented and maintained in accordance with the CDSA *APCP: Content Protection and Security Standards and Procedures*,

- 1.3.c. review the content protection and security management system, at specified intervals, to ensure its continuing effectiveness, and to identify opportunities for continual improvement (also see 1.4).
 - 1.3.d. initiate audits, corrective actions and preventive actions to minimize non-conformities relating to the CDSA *APCP: Content Protection and Security Standards and Procedures*,
 - 1.3.e. ensure the content protection and security policies comply with applicable legal, regulatory and client requirements, and
 - 1.3.f. contact the client and/or the relevant content owner or representative body of non-conforming situations.
- 1.4. Senior site management shall review the site's content protection and security management system, at specified intervals to ensure its continuing suitability, adequacy and effectiveness.
- 1.5. Inputs to the management review shall include:
- 1.5.a. the results of internal and external content protection and security management system audits and the status of corrective and preventive action(s),
 - 1.5.b. communications from customers, including security-related incidents,
 - 1.5.c. the assessment of the performance of the content protection and security management system, as well as security incidents,
 - 1.5.d. an assessment of recommended changes to the security management system, including the security policy and procedures,
 - 1.5.e. an assessment of changing conditions, including security exposures,
 - 1.5.f. follow up actions from previous management reviews, and
 - 1.5.g. an assessment of improvement opportunities and recommendations for improvement.
- 1.6. Outputs of the management review shall include any decisions made, action plans and/or recommendations related to the content protection and security management system. Outputs shall also include any changes made to the security policies and procedures to support continual improvement.

2. DOCUMENTATION REQUIREMENTS

- 2.1. The site shall establish, implement and maintain a content protection and security management system manual to document its systems, procedures, processes, policies, responsibilities and authorities, and its conformity to these CDSA *APCP: Content Protection and Security Standards and Procedures*.
- 2.2. The site shall establish, implement and maintain documented procedure(s) to control all documents related to the CDSA *APCP: Content Protection and Security Standards and Procedures*. Documents can be in any physical or electronic form. Records are a specific type of document and shall be controlled according to the requirements. The documented procedure shall identify methods for:
 - 2.2.a. ensuring that authorized personnel approve all documents prior to being issued,
 - 2.2.b. making document changes as a result of corrective action, preventive action, or other continual improvement of the security system,
 - 2.2.c. reviewing and revising documents to ensure their continuing suitability, accuracy and relevance,
 - 2.2.d. ensuring document changes and their current revision status are identified through suitable means, such as a master list, to prevent the use of invalid and/or obsolete documents. The reason for changes shall be recorded,
 - 2.2.e. ensuring that current documents are legible and readily retrievable at workstations, as appropriate,
 - 2.2.f. maintaining records to document conformance to these CDSA *APCP: Content Protection and Security Standards and Procedures* and to specific requirements of the content protection and security management system for a minimum of three years, with the exception of records that have another minimum retention period specifically defined in these CDSA *APCP: Content Protection and Security Standards and Procedures*,
 - 2.2.g. preventing the unintended use of obsolete documents by suitable means if they are retained for any purpose.

3. COMPLIANCE AND CONTINUOUS IMPROVEMENT

LAWS AND REGULATIONS

- 3.1. The site shall have access to information concerning laws and regulations relating to protection of intellectual properties.

- 3.2. The site's content protection and security management system policies and procedures shall comply with all applicable local and international laws and regulations relating to the intellectual property control, protection and security.
- 3.3. Applicable laws shall be periodically reviewed to ensure continued compliance and promote their communication to affected personnel.
- 3.4. In the event of a contradiction between the requirements of applicable laws and regulations and these CDSA *APCP: Content Protection and Security Standards and Procedures*, the laws and regulations shall have precedence.

RISK MANAGEMENT

- 3.5. The site shall establish, implement and maintain appropriate policies, preventive and/or mitigation controls commensurate with such risks by determining risks associated with all content, media, information assets, intellectual property and product within the scope of this standard and identify the impact on business operations, by:
 - 3.5.a. establishing a central risk management focal point to ensure all risks, controls and treatments are regularly reviewed and evaluated for any changes,
 - 3.5.b. implementing appropriate risk mitigation controls and updating policies and related controls, and
 - 3.5.c. monitoring and evaluating the effectiveness of implemented policies and controls.

RISK ASSESSMENT

- 3.6. The site shall identify potential sources of loss, damage, misuse and theft of assets in the content delivery supply chain, and evaluate the need for appropriate action(s) to prevent losses or mitigate risks, and/or enforcement.

The site shall establish, implement and maintain a documented risk assessment procedure that includes methods to:

- 3.6.a. define the roles and responsibilities of personnel performing risk assessments,
- 3.6.b. identify the potential risks associated with factors such as the nature of the content and its transmission; processes for handling, storage and delivery; media formats; personnel; technology; facilities; and processes within the scope of this Standard that it can control and those that it can influence taking into account planned or new customer projects, or new or modified activities, products and services,
- 3.6.c. determine and rank the significance and probability of risks that have or can have impact(s) on the unauthorized accessibility, use, integrity, security and confidentiality of customer's intellectual property and related assets, using appropriate tools and techniques,

- 3.6.d. prioritize risk factors on the basis of their significance, the probability and impact of threats and vulnerabilities (e.g., personnel, facilities and equipment, software and operating systems, access, technology, etc.), the nature and scope of customer projects, the value of the intellectual property, potential financial and other internal and external business consequences that could result (e.g., financial loss, operational/productivity losses, loss of customer trust, loss of reputation in the industry, etc.),
- 3.6.e. ensure periodic reassessment of risks to address any changes to risks and threats and ensure the suitability, appropriateness and continuing effectiveness of the policies, mitigation methods, and controls,
- 3.6.f. communicate the results of risk assessment(s) and reassessment(s) to management for appropriate action, and
- 3.6.g. monitor, measure and analyze the process, and implement actions necessary to achieve objectives and continually improve the risk assessment process.

The site shall record and maintain the results of the risk assessment and keep it up to date.

Where a site chooses to subcontract any activities that may affect the protection, integrity or security of customer content, the site shall include such activities in the risk assessment to ensure appropriate control over such processes. Contracts with subcontractors shall include commensurate performance requirements and conditions to ensure appropriate control of customer content.

GAP ANALYSIS

- 3.7. The site shall analyze the effectiveness of existing or proposed policies, mitigation methods and controls required to ensure risk management processes are effective. The site shall establish, implement and maintain a documented procedure of a gap analysis process to:
 - 3.7.a. identify the roles and responsibilities of personnel involved in the gap analysis process,
 - 3.7.b. gather information on existing policies and controls, the value of critical operations and assets, internal and external communication channels, and other system attributes and compare this information with existing policy and control requirements, and the requirements of these Standards. The site should consider other information, including cost-benefit information, impacts on the customer and impacts on the site's personnel,
 - 3.7.c. identify any gaps between policies and controls, organizational objectives and other requirements, to determine feasibility to address the gaps, and recommend feasible solutions to correct the gaps,
 - 3.7.d. communicate the results of the gap analysis to management,

- 3.7.e. approve the controls to be implemented to address the identified gaps and related action plans by responsible management,
- 3.7.f. document and approve decisions not to address gaps on the basis of business priorities, customer, operational and/or other considerations, and identify existing compensating controls where needed, and
- 3.7.g. monitor and assess the implementation and effectiveness of action plans to address identified gaps.

The site shall record and maintain the results of gap analyses.

This section of these CDSA *APCP: Content Protection and Security Standards and Procedures* is not intended to preclude customer contract reviews, customer audits, or other imposed customer requirements.

RISK MITIGATION

- 3.8. The site shall take appropriate action to mitigate identified risks, establish and maintain a management processes for:
 - 3.8.a. implementing new or improved policies and related controls resulting from risk assessment, risk level assignments, gap analysis and related action plans,
 - 3.8.b. promoting awareness at appropriate levels of the site's organization and encouraging employees' active participation by submitting suggestions and observations to identify and mitigate risks,
 - 3.8.c. ensuring that a mechanism exists for staff to report suspicions, events and other security concerns anonymously and a policy exists whereby staff can report such issues and name individuals without fear of reprisal or other prejudicial action by management or colleagues. Malicious or intentionally divisive reports are not to be afforded such treatment.
 - 3.8.d. ensuring resources/budgets are allocated by top management to mitigation activities,
 - 3.8.e. developing mitigation plans which include the steps to be taken, the expected completion schedule, the responsible personnel involved, actions to be implemented and methods for monitoring implementation action plans,
 - 3.8.f. ensuring that the implementation strategy is determined, defined, approved, communicated and implemented at appropriate levels of the site's organization, and
 - 3.8.g. assessing new or modified policies and/or controls to ensure that they are properly and effectively implemented so that the risk exposure no longer exists or the risk has been sufficiently reduced. If risk mitigation needs are not met, the site shall take appropriate action and follow-up.

RISK MONITORING AND EVALUATION

- 3.9. The site shall take appropriate action to ensure the effective implementation of mitigation activities. The site shall establish, implement and maintain a documented procedure to ensure that:
- 3.9.a. the process for monitoring and evaluating the policy and control measures is effective.
 - 3.9.b. the mitigation plan and policy reviews are performed periodically and at the appropriate level of the site's organization, according to planned schedules.
 - 3.9.c. when significant operational changes occur that affect risk to customer content – e.g., relocation of departments or facilities, revision of operational services or technology – the risk mitigation activities, policies and procedures shall be reviewed, revised and documented.

ON-GOING MONITORING AND INCIDENT REPORTING

- 3.10. The site shall establish, implement and maintain a process to monitor on a regular basis security incidents and characteristics of its activities that can have a significant negative impact on content protection and security. The procedure shall include the documentation of information to monitor performance, operational controls and conformity with the site's content protection and security policy.
- 3.11. The site shall establish, implement and maintain a procedure for handling actual or potential security breaches. The procedure shall define requirements for:
- 3.11.a. identifying the type of security incident (e.g., theft, premature release, loss of customer intellectual property and related assets, etc.),
 - 3.11.b. identifying details about the security incident, including the nature of the incident, date, time and location of incident, and those involved in the incident,
 - 3.11.c. investigating security incident incidents and their root causes,
 - 3.11.d. characterizing the significance and impact of the actual or potential loss,
 - 3.11.e. initiating immediate corrective action and/or preventive action as necessary,
 - 3.11.f. evaluating the need to considering security incident information in the risk management process (see sections 3.5 through 3.9.) based upon the significance and impact of the security incident, to continually improve the content protection and security system, and
 - 3.11.g. evaluating the effectiveness of any actions taken to address security incidents.

CORRECTIVE AND PREVENTATIVE ACTIONS

3.12. The site shall establish, implement and maintain documented procedures to ensure situations not conforming to requirements of these CDSA *APCP: Content Protection and Security Standards and Procedures* are documented.

3.13. The site shall establish, implement and maintain documented procedures, which ensure the documentation, implementation and effectiveness of corrective actions.

Actions taken should effectively eliminate the root causes of system non-conformities and prevent their reoccurrence. Corrective action shall be effectively implemented, fully communicated to all site personnel and implemented in a timely fashion. Any actions taken should be appropriate to the risks encountered and the effects on security.

3.14. The site shall establish, implement and maintain documented procedures, which ensure the documentation, implementation and effectiveness of preventative actions.

Actions taken should effectively eliminate the root causes of potential system non-conformities and prevent their reoccurrence. Preventive action shall be effectively implemented, fully communicated to all site personnel and implemented in a timely fashion. Any actions taken should be commensurate to the potential risks encountered and the effects on security

INTERNAL AUDITS

3.15. The site shall establish, implement and maintain internal auditing procedures to ensure content protection and security activities comply with these CDSA *APCP: Content Protection and Security Standards and Procedures*.

3.16. Personnel independent of those having direct responsibility for the activity being audited must carry out such audits and must be suitably qualified for such duties.

3.17. Results of the site's internal audits shall be recorded and reported to personnel having responsibility in the areas audited. Management personnel responsible for those areas shall immediately devise corrective actions on audit deficiencies. Follow-up activities shall verify and record the implementation and effectiveness of the corrective actions.

3.18. Results of the site's internal audits and a summary of the corrective and preventive actions planned and implemented shall be the subject of the next management review meetings (see section 1.5). The portion of minutes of these review meetings with conclusions, results and actions taken relating to compliance to the CDSA *APCP: Content Protection and Security Standards and Procedures*, shall be forwarded in writing to CDSA and to the CDSA-designated external auditor.

3.19. Within six months of being certified by CDSA, site personnel shall conduct an internal audit to ensure continued compliance to these Standards and Procedures. A report of the findings

of the internal audit and the resulting corrective actions shall be made in writing to CDSA and the designated external auditor. Site personnel shall conduct similar internal audits at least once a year, but no sooner than six months after the last external audit and no later than 60 days before the next external audit, to ensure continued compliance to these Standards and shall report findings of these audits and the resulting corrective actions to CDSA and the external auditor.

EXTERNAL AUDITS

3.20. An auditor retained by CDSA will audit procedures and documentation after the implementation of the site's approved manual.

3.21. If the auditor determines that the site's systems do not comply fully with these Standards and Procedures, or is not fully implemented, the audit report will contain non-compliance reports. Non-compliances are classified as "minor" or "major", depending upon their severity.

A minor non-compliance is a non-systemic non-fulfillment of an element of a clause of these Standards and Procedures.

A major non-compliance is a systemic or repeated non-fulfillment of an entire clause of these Standards and Procedures.

3.22. If no non-compliances are found in an initial certification audit, the site shall be certified.

If only minor non-compliances are found in an initial certification audit, the site shall have 30 days to submit a corrective action report to the auditor. If the auditor judges the corrective action report acceptable, the site shall be certified.

In the case of major non-compliances found during an initial certification audit, the site, prior to the CDSA auditor returning for a required re-audit, must undertake a corrective action program. Successful completion of this re-audit (i.e., no major non-compliances) shall result in the site being certified.

3.23. The effective period for this initial certification is six months from the date of the initial audit unless the site is currently certified under another CDSA APCP system, in which case, the new certification is valid until the next regularly scheduled surveillance audit for the previously existing system certification.

3.24. At the end of the initial certification period the site must undergo an external surveillance audit performed by a CDSA auditor.

3.25. If no non-compliances are found in a surveillance audit, the site shall be certified for a twelve month period.

If only minor non-compliances are found in a surveillance audit, the site shall have 30 days to submit a corrective action report to the auditor. If the auditor judges the corrective action report acceptable, the site shall be certified for a twelve month period.

In the case of major non-compliances found during a surveillance audit, the site must undertake a corrective action plan. Depending on the nature and severity of the major non-compliances, CDSA reserves the right to require a re-audit. Successful completion of the corrective action program and possible re-audit (i.e., no major non-compliances) shall result in the site being certified for a twelve month period.

- 3.26. Thereafter, the site must undergo an annual external audit performed by a CDSA-designated auditor. In addition, the site must conduct its own internal audits (See Section 3.15).
- 3.27. CDSA reserves the right to conduct such external audits at intervals other than one year for specific reasons.
- 3.28. CDSA publicly acknowledges through presentations, advertisements, website listings and other methods, sites that have been issued a CDSA Anti-Piracy Certificate of Compliance.
- 3.29. If any major non-compliance revealed by an internal or external audit are not corrected, documented to CDSA and re-audited (as required in Section 3.25) within 30 days of discovery, CDSA reserves the right to suspend certification until appropriate corrective actions are implemented and, at CDSA's option, to publicly acknowledge such suspension.
- 3.30. If an external audit or re-audit is not performed within 30 days of the scheduled date, CDSA reserves the right to suspend certification, and, at CDSA's option, to publicly acknowledge such suspension.

4. TRAINING AND AWARENESS

- 4.1. The site shall establish, implement and maintain a procedure for training personnel performing activities affecting content protection and security. The procedure shall identify the nature of the training and training needs.
- 4.2. Personnel performing tasks affecting content protection and security shall be qualified on the basis of education, training and/or experience.
- 4.3. Records of all such training shall include at a minimum the topic, date, place of training, instructor(s) and the names of individuals trained, plus other information.
- 4.4. Contractors with responsibilities related to content protection and security (e.g., cleaning staff and guards) shall be sufficiently trained to meet the requirements of these CDSA *APCP: Content Protection and Security Standards and Procedures*.
- 4.5. All site personnel, regardless of their responsibilities, shall be informed of the content protection and security policy (see section 1.2).

5. SITE SECURITY

SITE PERIMETER

- 5.1. A secure perimeter shall be defined for the site. The secure perimeter may not necessarily be the site boundary, but shall include all areas where client's assets and products are normally present.
- 5.2. All site employees and contractors must present identification badges, key cards or similar upon entering the secure perimeter. (See Section 9.8 for screening visitors' possessions.)

The site shall have a system to authorize entry in the event the employee or contractor is not carrying the proper badge or key card. Under no circumstance is it acceptable to allow entry only based upon sight recognition of an individual.

- 5.3. The site shall establish, implement and maintain procedures for authorizing, issuing, retrieving and replacing identification badges, physical keys and electronic access keys (e.g., swipe cards/proximity devices.) This shall also include a system to alert security personnel of the termination of employees.
- 5.4. Visitors must register before entering the secure perimeter and be escorted at all times. Visitors must provide photo identification prior to entry. In addition to their name and company, entry time, date and authorizing person must be recorded.

MONITORING AND CCTV

- 5.5. A combination of fences, guards, locks (physically or electronically activated), alarms, motion detectors and closed-circuit television (CCTV) cameras may be used to restrict and monitor personnel and product access in and out of the secure perimeter.
- 5.6. Lighting must be sufficient for guards and CCTV systems to be effective. In lower traffic areas, lights may be activated by motion detectors in order to save energy.
- 5.7. Video image quality should be of an evidential standard and capable of fulfilling the control objective of clearly identifying in-field-of-view events, persons and objects in motion or still.
- 5.8. Video images captured by the CCTV system must be retained for a minimum of 30 days. The video images may be stored on tape, hard drive, or other format. Regardless of the format, retained video data must be securely and safely stored in such a way as to reasonably prevent loss, theft, or deletion.

ENTRY AND EXIT

- 5.9. All persons (employees, contractors and visitors) and their possessions shall be subject to search upon exit from the site's secure perimeter. Any search should be thorough enough to detect client assets and products in either physical or electronic form.

Searches may be performed universally or randomly. If random searches are applied, the method for determining who will be searched must be documented and applied without exception. Also, the frequency of random searches must be sufficient to represent a meaningful deterrent to theft.

It is strongly recommended that contractors and visitors to the site be informed of the search policy prior to entry. It is also advisable to have contractors and visitors declare items in their possession that might potentially cause difficulties upon exit. Such items might include optical discs (pre-recorded or recordable), computers, personal storage devices, or samples.

- 5.10. Personnel performing the searches shall be trained to recognize assets and products in electronic and physical forms.
- 5.11. The site shall establish, implement and maintain procedures for responding to cases of possible theft detected by exit searches, video surveillance or other methods (also see section 3.10.)

BACKGROUND CHECKS

- 5.12. Where local law permits, it is recommended site management conduct background checks on personnel, especially for individuals frequently exposed to pre-release assets or with security responsibilities.

6. ELECTRONIC DATA

COMPUTER USE

- 6.1. The site shall have a computer use policy to inform personnel of expectations regarding proper, professional use of computer resources. The policy shall also inform personnel of the possible risks and consequences for improper use of computer resources.
- 6.2. Username and passwords should be required to login on to computer systems, whenever possible. Individual users should have unique login details; group usernames and passwords should be avoided.

Login passwords shall be changed regularly.

Access to user and password data shall be strictly controlled and limited to authorized personnel.

- 6.3. Computers storing or processing client assets should be not connected to the internet or other networks, whenever possible. Internal networks containing client assets are permitted, but should remain isolated from the internet and other external networks.

- 6.4. The site must have systems to restrict and monitor off-site electronic file transfers from all computers connected to the internet or other external networks.

E-mail restrictions might include limited file size, prohibition of certain attached file type, and/or logging and monitoring of messages with attachments sent to suspicious or unknown addresses.

Transfers to internet sites, FTP sites or through other delivery systems can be restricted and monitored through firewall configurations.

- 6.5. Client assets received electronically should not remain in user local inboxes or drives for an extended period of time. Whenever possible, assets should be transferred to physical media or a designated, secure network drive location.
- 6.6. The use of specialized systems for encryption, decryption or marking of incoming client asset data must be limited to authorized personnel.

PERSONAL STORAGE DEVICES

- 6.7. The site shall have written policies regarding the possession and usage of personal storage devices (USB memory sticks, PDA's, MP3 players, etc.). It is recommended such devices be generally prohibited and formally authorized only in limited situations.

Personnel conducting exit searches (see Section 5.9) must be informed of the risk posed by such devices and trained to recognize them.

- 6.8. Employee's personal copies of electronic files should not be stored on the site's computer systems, except where there is no reasonable possibility to confuse them with clients' assets.
- 6.9. The site shall establish, implement and maintain procedures for responding to cases of actual or potential theft, loss or exposure of electronic assets (also see section 3.10.)

7. ASSET HANDLING AND STORAGE

ASSET ID AND TRACEABILITY

- 7.1. The site shall identify all classes of assets and products to which these Standards and Procedures are applicable. Assets may be in electronic or physical form. At a minimum, the assets and products shall include customer-supplied master data sources, stampers, finished products and packaging materials designed to prove product legitimacy (e.g., hologram stickers and authenticity certificates).
- 7.2. All handling, processing and storage of the assets and products must be within the site's secure perimeter (see Section 5.1), except for immediate receipt and dispatch.

- 7.3. The site shall establish, implement and maintain procedures for logging and transferring assets and products from the point of receipt to authorized personnel.
- 7.4. The site shall establish, implement and maintain procedures for tracking and counting (to a reasonable degree of accuracy) assets and products in process.
- 7.5. Physical assets and products stored for longer periods (i.e., not work in process) shall be included in an inventory control system with tracking of movement into and out of the storage area. The inventory must be subject to regular cycle counts to confirm accuracy.

Small quantities of product retained for purposes such as quality samples may be exempted from the cycle count requirement. However, the product should be stored in a specifically designated area within the site's secure perimeter.

- 7.6. If the inventory cycle count reveals missing items or other irregularities, and immediate attempts to reconcile the inventory fail, a non-conformance report shall be initiated. If the non-conformance system determines there is any reasonable possibility the assets or products have been removed from the site, the related client must be informed.
- 7.7. The site shall establish policies regarding the storage of products in offices and other areas not directly related to the process. The decorative display of products should be generally prohibited and only allowed in limited designated areas.

ASSET TRANSPORT

- 7.8. Records must be kept of the off site movement of assets or products to other vendors or services providers. Examples may include editing studios, authoring houses and packaging operations.
- 7.9. Off site vendors and service providers must be vetted to ensure reliability and that reasonable security measures are in place, except when the client requires a specific vendor or service provider or the site is reasonably certain the vendor or service provider is reliable and has taken reasonable security measures.
- 7.10. Records must be kept of the return of all assets and products to clients or their designated agents.
- 7.11. The site shall establish, implement and maintain a procedure to document and authorize the removal from the site of any asset or product (or any item which could be mistaken for a real asset or product) by any employee, contractor or visitor.
- 7.12. Couriers of assets and products must be vetted to ensure reliability and adequate shipment tracking capabilities are in place, except when the client requires a specific courier or the site is reasonably certain the courier is reliable and capable of tracking shipments. Suitable Service Level Agreements (SLA) must be executed by all couriers, including subcontractors, used for transport and shipment of assets.

ASSET DISPOSAL

7.13. Records must be kept of the disposal of all assets and products.

7.14. All assets and products to be disposed of must be destroyed or rendered useless before removal from the site.

Removal from the site prior to destruction may be allowed only by specialist contractors using secure transport directly to the destruction contractor site where the assets will be destroyed or rendered useless under strictly controlled and secure conditions. A Certificate of Destruction, or similar suitable document must be issued by the destruction contractor and maintained at the site.

7.15. The site shall establish, implement and maintain procedures for responding to cases of actual or potential theft or loss of assets (also see section 3.10.).

DECLINATION OF LIABILITY

CDSA has made every effort to formulate a standard that it believes will help sites reduce the likelihood of loss or theft of media-related assets in electronic and physical form. However, a standard, no matter its specificity or diligent application, cannot guarantee avoidance of a claim. Therefore, CDSA must decline any liability toward a content owner, manufacturer, or third party on account of this standard, whether or not CDSA has issued a certificate of compliance.

GLOSSARY

Anti-Piracy and Compliance Programs (APCP) – A comprehensive set of program standards designed to provide content supply chain security at media creation, manufacturing, storage and delivery supply chain sites. Compliance is applied through comprehensive internal security risk management assessments and stringent operational procedures and ongoing external audits by independent ISO accredited auditors.

Asset – Any tangible or intangible intellectual property, information, work in process or final product in the supply chain from content creation, production, digital compression, encoding and authoring to manufacturing and distribution of final product that has value to an organization, its customers, or an intellectual property rights owner. An asset may also take a digital or electronic form.

Audit – A documented activity to verify by examination and evaluation of objective evidence that applicable elements of the APCP standards are suitable and have been developed and implemented by the audited site in accordance with specified APCP requirements. Within the APCP, required audits are conducted internally by the site and externally by independent ISO accredited auditors selected by CDSA. Successful external audits lead to a site's certification and periodic re-certification under the APCP.

Content Delivery & Storage Association (CDSA) – The worldwide forum advocating the innovative and responsible delivery and storage of entertainment, software and information content which develops, administers, and maintains the Anti-Piracy and Compliance Programs (APCP).

Control – Any administrative, management, technical, or legal method, and safeguards used to manage risk and to protect assets. Examples of a control are policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

Corrective Action – A change implemented to address a nonconformity or failure identified in a management system which is taken to correct and/or prevent recurrence of the root cause of the condition that caused the nonconformity or failure.

Countermeasure – Any action taken to mitigate a negative risk or effect.

Digital Asset Management – Process of capturing and managing media and asset files (e.g., media, graphics, audio, video, etc.) so they can be revised, repurposed, and/or accessed.

Documentation – Information and the medium that is used to bring it into existence.

Gap Analysis – An examination of information on existing policies and controls, the value of critical operations and assets, internal and external communication channels, and other system attributes and compare this information with existing policy and control requirements, and the requirements of these Standards to identify variances between policies and controls, organizational objectives and other requirements, to determine feasibility to address the gaps, and recommend feasible solutions to correct the variances

Integrity – Veracity, confidentiality, accuracy, and completeness of assets and /or intellectual property through methods used to process and manage it.

Intellectual Property – Any original, tangible property or creative work which is protected by law (e.g., by copyright, trademark, etc.) from being used without specific permission of the owner.

Organization – An established entity with a defined management and personnel structure, scope of operations, and services and/or products, and for purposes of the APCP, conducting business within the content delivery and storage industry.

Physical Asset Management – Appropriate policies, controls and procedures to reduce risks and enhance security of content entrusted to the supply chain service provider.

Preventive Action – A change implemented to address a weakness in a management system that is not yet responsible for causing nonconforming product or service.

Residual Risk – Threat that remains after instituting a selected risk treatment (i.e., acceptance of the risk, avoidance of the risk, transference of the risk, or reduction of the risk).

Risk – The probability of the occurrence of a threat (i.e., of loss, damage, misuse, or theft)

Risk Assessment – Process for identifying potential sources of loss, damage, misuse and theft of intellectual property in the content delivery supply chain, identify risk exposures, and evaluate the need for appropriate action(s) to prevent losses or mitigate risks, and/or enforcement. (See Addendum – page 19.)

Security Perimeter – A delineated boundary comprised of barriers such as walls, card controlled entry gates, security surveillance and manned entry points which is used to restrict access to protected areas that contain assets, products, related materials, information, and asset processing operations.

Security Incident – An actual or potential security breach which may result in a loss of asset integrity, confidentiality, damage, misuse, or theft.

Security Policy – A statement of management’s commitment to the implementation, maintenance, and improvement of its information security management system.

Security System – The set of security measures, policies, procedures and safeguards to protect intellectual property, which is suitable for an assessment by an external party.

Site – The place where the organization maintains assets and related materials, and otherwise conducts business related to the security management system.

Site Perimeter – The defined, physical or digital boundary of the site’s location, its systems and networks, which defines the inside and outside of where assets are present.

Supply Chain – The managed delivery mechanism for transferring intellectual property and similar content in physical and electronic forms from point to point as an integrated stages of the content delivery system.

GLOSSARY ADDENDUM
RISK MANAGEMENT – ASSESSMENT – MITIGATION SYSTEM

