



---

**CONTENT DELIVERY AND STORAGE ASSOCIATION  
ANTI-PIRACY AND COMPLIANCE PROGRAMS**

**CONTENT PROTECTION AND SECURITY  
DIGITAL DOWNLOAD SUPPLY CHAIN  
STANDARDS AND PROCEDURES, VERSION 1**

---

## **Table of Contents**

1. INTRODUCTION.....	1
2. SITE PERSONNEL AND RESOURCES.....	3
3. DOCUMENTS AND DATA CONTROL .....	4
4. RISK MANAGEMENT .....	5
5. NON-CONFORMANCES & PREVENTIVE ACTIONS .....	8
6. RECORDS .....	8
7. INTERNAL AUDITS .....	9
8. EXTERNAL AUDITS .....	9
9. TRAINING .....	11
10. SITE SECURITY .....	13
11. ELECTRONIC DATA .....	14
12. ASSET HANDLING AND STORAGE .....	17
13. PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS.....	18
DECLINATION OF LIABILITY .....	18

## **Addenda**

Addendum 1:	
Risk Management – Assessment – Mitigation System .....	19
Addendum 2:	
Content Security Management System .....	21
1 Security Policy .....	21
2 Roles and Responsibilities .....	21
3 Document Control.....	21
4 Site Exit and Entry Control .....	22
5 Site Secured Area Control.....	23
6 Camera Monitoring and Maintenance.....	24
7 Content Transmission Control and Monitoring.....	24
8 Content Access Control and Monitoring.....	25
9 Media Access Control and Monitoring .....	26
10 Device Control and Monitoring .....	26

---

## 1. INTRODUCTION

---

1.1 The Digital Download Supply Chain Standards & Procedures (Standards and Procedures) is part of the Content Delivery & Storage Association's Anti-Piracy and Compliance Programs (APCP), an industry-driven initiative designed to protect intellectual property in the supply chain from content creation, production, digital compression, encoding, and authoring to manufacturing and distribution of final product. These Standards and Procedures have been developed by a task force representing Intellectual Property Owners, their Manufacturers, Suppliers and Distributors along the content delivery supply chain. This policy is to be understood and maintained by all levels of the organization involved with these Standards and Procedures.

1.2 The objective of these Standards and Procedures is to provide a framework for managing assets assigned to digital download supply chain partners of client content owners in a managed manner and by reducing risks to levels acceptable to the content owner by:

- a. Reducing the chances of unauthorized digital downloads through security leaks within the storage and distribution channels of the content owners' supply chain partners;
- b. Identifying loss of income and content assets through theft or unreported download sales; and
- c. Preventing or mitigating the loss of assets upon the cessation of the business relationship between the content owner and a download supply chain partner.

1.3 These Standards and Procedures specify the minimum technical and procedural requirements for protection of client assets and products by organizations and facilities providing services within the Digital Download Supply Chain, including, but not limited to:

- a. Creative production of content,
- b. Compression, encoding, and authoring of content, and
- c. Storage and distribution of content by digital means,
- d. Adherence to copyright laws and processes.

These Standards and Procedures are subject to review and modification as relative technology, industry practices, and other aspects affecting content protection and security of digital downloads evolve.

1.4 These Standards and Procedures are suitable for the assessment of the content security management system of the organization by an external party. They represent the essence of good business practices tailored specifically to content creation and delivery. These Standards and Procedures were designed to complement the ISO 9001 quality management standard, and the ISO 17799 and ISO 27000 series standards for information security.

1.5 Sections 2 through 10 of these Standards and Procedures describe the primary, broad internal procedures and requirements. Sections 11 through 13 describe specific technical requirements that must be in place in order for a site to be compliant with these Standards and Procedures.

16 For the purposes of interpreting this document, the following definitions apply:

- a. **Organization.** An organization is a single business entity, comprised of one or more varied functions, which was created to accomplish a common set of goals. An organization may be comprised of one or more sites.

- b. **Site.** A site is a single geographical location of an organization, which participates in the digital download and content security system activities. Although there might be other organizations or functional areas unrelated to the digital download and content security system located within one site, it must be demonstrated that these entities are prevented from interfering with the effective operation content security management system or accessing digital content, unless duly authorized.
- c. **Scope.** The scope is range of functions and activities encompassed in the digital download and content security management system. The scope also defines the areas of the organization included in the content security management system as well as its boundaries, in terms of:
  - i. the purpose and characteristics of the organization,
  - ii. its site location(s) and its identified physical and information systems perimeter(s) that operate in compliance with these Standards and Procedures
  - iii. the assets and technology utilized, and
  - iv. any functional exclusions, which are outside of the boundaries of the digital download supply chain.
- d. **Supply Chain.** A supply chain is the collection and sequence of functions and activities that manage the creation, production and distribution of physical and digital assets. The supply chain is comprised of an organization and its suppliers and subcontractors involved in producing, handling and/or distributing such assets.

---

## 2. SITE PERSONNEL AND RESOURCES

---

2.1 The Digital Download Supply Chain Standards & Procedures (Standards and Procedures) are designed to protect intellectual property in the storage and electronic distribution of digital content adherence to the procedures and guidelines set forth in this document. This purpose must be understood and upheld by all levels of personnel within organizations involved with the CDSA Anti-Piracy and Compliance Programs.

2.2 Organizations must document and specify the security requirements and procedures for each of their sites as outlined in these Standards and Procedures. All staff members are expected to read and understand these requirements.

2.3 A statement must be signed by each employee within the organization or site, and the signature witnessed (or notarised) to ensure the employee agrees to abide by the security requirements, is fully aware of the seriousness of his commitment to the integrity of data and other material handled, and understands the consequences to the company and employee when a security breach occurs. All employees should be made aware that the organization is required to take immediate corrective action when a person employed by the company is found and proved to have been in breach of these security requirements.

2.4 The responsibilities 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:

- a. Initiate any preventive actions to avoid non-conformities relating to the CDSA Anti-Piracy Standard.
- b. Identify problems and recommend, initiate, provide and verify solutions.
- c. Contact the customer and/or the relevant content owner or representative body of non-conforming situations.

2.5 Organization management shall:

- a. Appoint a program manager who shall ensure that at each site systems, procedures, processes and documents are established and maintained in accordance with the CDSA Anti-Piracy and Compliance Programs. The program manager shall report performance against this standard for management board review. For multiple sites, particularly if geographically widespread, consideration should be given to the appointment of subordinate staff who report to the program manager.
- b. Identify and provide resources for control, work performance and verification, including audits.
- c. Review system performance at specified intervals as agreed the certification process to ensure continuing system effectiveness. Such performance reviews shall be documented, with records kept in accordance with these Standards and Procedures and shall take place at least annually.

2.6 Each site shall establish and maintain a site manual to document its systems, procedures, processes, policies, responsibilities and authorities, and its conformity to these Standards and Procedures.

---

### 3. DOCUMENTS AND DATA CONTROL

---

3.1 The organization shall establish and maintain documented procedures to control all documents that relate to these Standards and Procedures. The organization shall establish, implement and maintain documented procedure(s) to control documents that relate to the requirements of this Standard. Records are a specific type of document and shall be controlled according to the requirements of this section. The documented procedure shall identify methods for

- a. approval of documents for adequacy prior to issuance and distribution,
- b. ensuring changes and the current revision status are identified,
- c. reviewing and revising of documents as necessary,
- d. making document changes as a result of corrective action, preventive action, or other continual improvement of the content security system,
- e. ensuring documents remain legible and are easily identifiable,
- f. ensuring changes and the current revision status of documents are identified through suitable means such as a master list,
- g. accessing current versions of applicable documents at points of use,
- h. storing, maintaining and distributing documents as necessary, and
- i. preventing the unintended use of obsolete documents by suitable means if they are retained for any purpose.

3.2 Documents can be in paper or electronic form and must take account of the environmental conditions at each site.

3.3 The organization shall identify authorized personnel responsible for approving all documents prior to being issued. The same personnel authorized for original approval shall approve changes to these documents. The reason for the changes shall be recorded.

3.4 Documents shall be reviewed at least annually to ensure their continued accuracy and relevance. Documents shall be revised as necessary.

3.5 A master list of documents, identifying the current revision status of each document, shall be available to prevent the use of invalid and/or obsolete documents.

3.6 Appropriate documents shall be available at all appropriate workstations and a complete master original shall be held and controlled by the program manager or designate.

---

## 4. RISK MANAGEMENT

---

### GENERAL

4.1 Risk Management is the application of processes, procedures and technical control measures intended to reduce the opportunity and chance of an identified vulnerability or weakness being exploited to the detriment of the business. At its core lie the notions of ownership and management; each identified risk should be ‘owned’ by an organization or individual for whom the consequences of the risk becoming reality would have significant business impact. In all events, the risk owner has a veto on any given risk management strategy and should be able to articulate the degree of risk 3<sup>rd</sup> parties are allowed to manage on the risk owner’s behalf. This is often referred to as ‘Risk Allowance.’

4.2 Responsibility for the management of risk shall be aligned within an organization such that each level of risk manager has the budgetary and management authority to reduce risk by the application of countermeasures, whether they be technical or procedural. There is little value in expecting a risk owner to devolve management responsibility to an entity with no authority, especially since this will send a clear message back to the owner regarding the importance with which their asset is viewed within the organization.

4.3 Digital media content risk ownership shall rest with the original owning organization such as a record label, games and business software publisher, or film studio. The organization receiving the digital content shall agree in advance with the owner the amount of flexibility allowed in managing the risks of loss or other compromise of the material. When Service Level Agreements (SLA) exist to address such responsibilities as content availability, access, risk ownership and assignment, liability, system requirements, outsourcing, data trading, inventory management, performance and other services, the organization shall document the implementation and maintenance of the SLA.

4.4 The organization shall identify, document, implement and maintain risk management procedures to protect the confidentiality, integrity and availability of customer intellectual property and related assets through content production, compression, encoding, authoring, storage and content delivery, as applicable to the nature of the business relationship.

4.5 The organization shall determine, implement and maintain appropriate policies, preventive and/or mitigation controls aimed at achieving the protection of confidentiality, integrity and availability by identifying risks associated with all content, media, information assets, intellectual property, and other related products falling within the scope of this standard and existing Service Level Agreements, as appropriate. They shall then determine the impact of those risks on business operations, by:

- a. establishing a senior risk management focal point to ensure all risks, controls, and treatments are regularly reviewed and evaluated for any changes
- b. implementing, possibly through lower-level management, appropriate risk mitigation controls, policies and related procedures
- c. monitoring and evaluating the effectiveness of implemented policies and controls.
- d. identifying areas where a management control is ineffective, or is not possible without severe restriction on business output, and reporting it to the risk owner for arbitration.

*N.B. A Risk Management schematic is provided in Addendum 1.*

### RISK ASSESSMENT

4.6 The organization shall identify those assets for which they have been given management responsibility on behalf of the owner. They shall identify potential sources of loss, damage, misuse and theft of intellectual property in the content delivery supply chain, and evaluate the need for appropriate action(s) to prevent losses, mitigate risks, and/or enforce some form of penalty where appropriate.

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

- a. define the roles and responsibilities of personnel performing risk assessments,
- 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. Planned or new customer projects, or new or modified activities, products and services must also be taken into account,
- 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,
- 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.),
- e. ensure annual 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,
- f. communicate the results of risk assessment(s) and reassessment(s) to the risk manager for appropriate action, and
- g. monitor, measure and analyze the risk assessment process, and implement actions necessary to achieve objectives and seek to continually improve the risk assessment process.

4.8 The organization shall record and maintain the results of the risk assessment and keep it up to date by recording where risk management strategies are considered to have altered the severity of the risk as originally defined in the assessment.

4.9 Where an organization chooses to subcontract any activities that may affect the protection, integrity or security of customer content, the organization 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

4.10 The organization shall analyze the effectiveness of existing or proposed policies, mitigation methods, and controls required to ensure risk management processes are effective. A procedure shall document, implement, and maintain a gap analysis process to:

- a. identify the roles and responsibilities of personnel involved in the gap analysis process,
- 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 this Standard. The organization should consider other information, including cost-benefit information, impacts on the customer, and impacts on the organization's personnel,
- c. identify any gaps between policies and controls, organizational objectives and other requirements, to determine the feasibility addressing the gaps, and recommend feasible solutions to correct the gaps,

- d. communicate the results of the gap analysis to the risk manager, and
- e. monitor and assess the implementation and effectiveness of action plans to address identified gaps.

4.11 The organization shall record and maintain the results of gap analyses in the same manner as for the risk assessment.

4.12 *This section of this Standard is not intended to preclude customer contract reviews, customer audits, or other imposed customer requirements.*

## RISK MITIGATION

4.13 Risk mitigation strategies fall into 4 main categories; remove, reduce, transfer or accept. These are discussed further in Addendum 1. Some strategies can be costly and impact on staff performance or business output. For this reason the senior risk manager should be a person in authority within the organization as discussed in 4.2. All mitigation measures should be discussed with, and approved by, the risk manager prior to their implementation. From a corporate governance perspective, the senior risk manager has the status of a trusted agent acting on behalf of the risk owner and this single fact should guide their decisions. The risk manager has direct responsibility for:

- a. approving the controls to be implemented to address any identified risks and corresponding gaps,
- b. approving any related action plans,
- c. documenting and approving 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
- d. articulating and addressing such shortfalls back to the risk owner where such shortfalls are outside the agreed SLA.

4.14 The organization shall take appropriate action to mitigate identified risks, establish and maintain a management processes for:

- a. implementing new or improved policies and related controls resulting from risk assessment, risk level assignments, gap analysis, and related action plans,
- b. promoting awareness at appropriate levels of the organization and encouraging employees' active participation by submitting suggestions and observations to identify and mitigate risks,
- c. ensuring resources/budgets are allocated by top management to allow mitigation activities to be undertaken by the risk manager,
- d. 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,
- e. ensuring that the implementation strategy is determined, defined, approved, communicated and implemented at appropriate levels of the organization, and
- f. 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 organization shall take appropriate action and follow-up.

## MONITORING AND EVALUATION

4.16 The organization shall take appropriate action to ensure the effective implementation of mitigation activities. The organization shall document a procedure to ensure that:

- a. The process for monitoring and evaluating the policy, and control measures, is effective,
- b. the mitigation plan and policy reviews are performed at least annually and at the appropriate level of the organization, according to planned schedules, and
- 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 as part of the operational change process, as opposed to a follow-on activity after the change.

---

## 5. NON-CONFORMANCES & PREVENTIVE ACTIONS

---

5.1 The organization shall establish, maintain and implement documented procedures to ensure situations not conforming to requirements of these Standards and Procedures are documented. Such non-conformances shall be scrutinized by the risk manager to assess their severity and impact.

5.2 The organization shall establish, maintain and implement documented procedures, which ensure the documentation, implementation and effectiveness of corrective and preventive actions.

---

## 6. RECORDS

---

6.1 Records shall be maintained to document conformance to these Standards and Procedures, including all exceptions noted.

6.2 Records shall be maintained a minimum of three years, except for some record types where a shorter retention period is specifically defined in these Standards and Procedures.

6.3 Such records shall be legible and readily retrievable. Records may be in paper or electronic formats. Where electronic formats are used, these should be version controlled and locked against alteration once published. The used of digital signatures for electronic documents is highly recommended.

---

## 7. INTERNAL AUDITS

---

7.1 Each site shall establish, maintain and implement internal auditing procedures to ensure that content protection and security activities comply with these Standards and Procedures.

7.2 The organization shall empower the program manager to schedule internal audits.

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

7.4 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.

7.5 Results of the site's internal audits, and a summary of the corrective and preventive actions planned and implemented shall be forwarded to the organization's risk manager and shall be included on the agenda of the next management review meeting (see section 2.5). The portion of the minutes of these review meetings with conclusions, results and actions taken relating to compliance to the CDSA APCP, shall be forwarded in writing to CDSA and to the CDSA-designated external auditor.

7.6 Within six months of being certified by CDSA, a site audit shall be carried out 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.

---

## 8. EXTERNAL AUDITS

---

8.1 Independent auditors, retained by CDSA, shall audit procedures, practices, environmental circumstances and documentation after implementation of the organization's or site's approved manual.

8.2 If the auditor determines that the content protection and security 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 shall be classified as "minor" or "major", depending upon their severity.

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

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

8.5 Where non-compliance falls between these two extremes, for example a repeated non-fulfillment of an element of a clause, external auditors will discuss it with site management to reach a consensus regarding its severity rating.

8.6 If no non-compliances are found in an initial certification audit, the site shall be certified. The effective period for this certification is six months from the date of the audit unless the site is currently certified under another APCP system, in which case, the new certification is valid until the next regularly scheduled surveillance audit for the previously existing system certification.

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

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

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

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

8.11 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.

8.12 In the case of major non-compliances found during a surveillance audit, the site must undertake corrective action. Depending on the nature 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.

8.13 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 in accordance with the provisions of Section 7.

8.14 The certification period shall be based upon the initial certification audit date. That is, the anniversary date for surveillance audits will be exactly 6, 18, 30, etc. months following the initial certification audit, regardless of the actual audit date of the previous surveillance audit or re-audit.

8.15 CDSA reserves the right to conduct such external audits at intervals other than one year for specific reasons. These reasons shall be notified in writing to the management of the controlling organization for sites where this proviso applies.

8.16 CDSA publicly acknowledges through presentations, advertisements, website listings and other methods, sites that have been issued a CDSA Anti-Piracy Certificate of Compliance.

8.17 If any major non-compliance revealed by an internal or external audit is not corrected, documented to CDSA, and re-audited (as required by Sections 8) within 30 days of discovery, CDSA reserves the right to suspend certification until appropriate corrective actions are implemented and, at CDSA's discretion, to publicly acknowledge such suspension.

8.18 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.

---

## 9. TRAINING

---

9.1 The site shall establish, implement and maintain procedures for training personnel performing activities affecting content protection and security; these procedures shall identify the nature of the training, the training needs and the standard to be attained.

9.2 Personnel performing tasks affecting content protection and security shall be deemed qualified for particular positions on the basis of education, training and/or experience relevant to that role.

9.3 Records of all such training shall be maintained for three years and shall include the topic, date, place of training, instructor(s), the individuals trained and the standard achieved, plus other information (e.g., length of time for the training period) at the discretion of the organization's management.

9.4 Contractors with responsibilities related to content protection and security (e.g., cleaning staff and guards) must also be sufficiently trained to meet the role they play in the organization's security model. This might take the form of induction training, periodic briefings or in-house awareness campaigns. Refresher training shall take place as warranted by technology changes, Service Level Agreements, policy – procedure revisions, risk management assessments, etc., but at least annually.

9.5 All the organization's personnel on site, regardless of their responsibilities, shall be informed of the systems and policies to protect client assets and products.

---

## 10. SITE SECURITY

---

10.1 A secure perimeter shall be defined for the site. The secure perimeter may not necessarily be the site boundary, but must include all areas where a client's assets and products are normally present or stored.

10.2 All site employees and contractors must present identification badges, key cards or similar upon entering the secured perimeter.

10.3 The site must 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.

10.4 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 must also include a system to alert security personnel of the termination of employees and the periodic changing of electronic keys to reduce the risks relating to key loss.

10.5 Sites must have a system for registering visitors before they enter the secured perimeter and they must be escorted at all times. Visitors must provide photographic identification prior to entry. In addition to their name and company, entry time, date, and authorizing person must be recorded.

10.6 Visitors possessions shall be subject to scrutiny prior to entering the site's secured perimeter. They shall be given an opportunity to surrender any physical or electronic devices that could be used to record client assets. Actual physical search may be warranted, but local legislation will dictate the feasibility of this. Where used, submitting to search should be a condition of entry inside the secure perimeter.

10.7 All persons (employees, contractors and visitors) and their possessions shall be subject to search by specifically appointed personnel upon exit from the site's secured perimeter. Any search should be thorough enough to detect client assets and products in either physical or electronic form. Ideally, the search should be conducted by persons who have no access inside the secured perimeter.

10.8 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.

10.9 It is strongly recommended that contractors and visitors to the site be informed of the search policy prior to entry.

10.10 Personnel performing the searches shall be trained to recognize assets and products in electronic and physical forms, and should have received training in the proper conduct of searches.

10.11 A combination of fences, guards, locks (physically or electronically activated), alarms, motion detectors, closed-circuit television (CCTV) cameras and other technological devices may be used to restrict and monitor personnel and product movement in and out of the secured perimeter.

10.12 Where used, all technical security measures must be demonstrably effective at achieving the aim for which they have been employed (i.e., CCTV must be able to identify objects sufficiently, guards must be able to patrol all necessary areas)

10.13 Video images captured by a CCTV system must be retained for a minimum of 30 days. 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.

10.14 The site shall establish, implement and maintain procedures for responding to cases of possible theft detected by exit searches, video surveillance or other methods.

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

10.16 As part of the internal audit process (See Section 7), the site shall review the adequacy of the security policy and methods as described and compare them with the implementation of the actual security practices, including periodic testing of them against real time events.

---

## 11. ELECTRONIC DATA

---

### INTERNAL USE AND PROCESSING

11.1 The site shall have a computer use policy to inform personnel of expectations regarding proper, professional use of computer resources. The policy should also inform personnel of the possible risks and consequences for improper use of computer resources.

11.2 Username and passwords combinations shall be required to login on to computer systems, whenever possible. Individual users shall have unique login details; group usernames and passwords should be avoided. Where group usernames and passwords are used, other controls shall be in place to achieve the adequate and suitable control and oversight as provided by individual login.

11.3 Login passwords shall be defined by a policy as to their length, complexity and the frequency at which they must be changed. The recommended complexity for passwords is a mix of letters, numbers and special characters (&\$\*@). The change frequency for passwords of less than 9 characters is 90 days.

11.4 Access to user and password data must be strictly controlled and limited to a system administrators.

11.5 Computers storing or processing client assets for internal use only shall be protected from the internet or other networks. Where connection to the internet cannot be avoided, client assets shall be stored within an encrypted area of the network. Where administrator accounts require connectivity to the internet, a separate account with normal user privilege shall be assigned for that purpose.

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

11.7 E-mail restrictions might include limited file size, prohibition of certain attached file types, and logging and monitoring of messages with attachments.

11.8 Transfers to internet sites, FTP sites or through other delivery systems shall be strictly controlled. Where such connection is necessary, it shall be restricted to as few individuals as possible and monitored through firewall configurations and accounting logs.

11.9 Client assets received electronically shall not remain in user local inboxes or drives for any longer than absolutely essential. Whenever possible, assets should be delivered by secure means as agreed by the content owner and transferred to secure storage under the control of a designated person as quickly as practicable.

11.10 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. Such exceptions shall be clearly documented and pointed out to the external auditor.

11.11 The use of specialized systems for encryption, decryption or marking of incoming client asset data must be limited to authorized personnel. Those individuals shall be formally identified and their roles clearly defined in the organization's risk management plans.

11.12 Employee's shall not store personal copies of electronic files site's computer systems. Where this is considered unfeasible, such files shall not be stored on any part of the system where clients' assets are also stored or processed.

## EXTERNAL USE AND PROCESSING

11.13 Organizations shall ensure that connections between their networks and any network external to them (including the internet) are adequately protected and monitored by the use of technical barriers. These barriers might include firewalls, Intrusion Detection or Prevention Systems.

11.14 Client assets authorized for digital downloads shall be maintained in a secure fashion where access is strictly controlled by electronic measures, including authorization codes, passwords, and similar verification systems.

11.15 Client assets no longer authorized for digital downloads shall be excluded from the download system either by technical means or by physical removal from the system. In either event they shall continue to be stored and secured in accordance with the procedures outlined in sections 11.1 through 11.14.

11.16 Authorized transmissions of client assets outside of the site shall be controlled by a system of checks and balances that include, at a minimum, traceable approval by designated managers; documentation of the transmission including the date, time, name(s) of asset(s) transmitted, size of file(s) transmitted, authorization number(s), and traceable identification of the recipient of the transmission (name, computer identification, address, etc.), and the identification of the site personnel and the computer transmitting the asset(s).

11.17 Authorized sales of client assets shall be documented and incorporated with the information required in Section 11.16 and include the purchase price, a traceable method of payment, and credit card processing codes, check number and other information, as appropriate.

11.18 Daily reconciliation of transmissions of client assets with information cited in Sections 11.16 and 11.17 and with the records of all transmissions to non-site locations shall be made and reviewed by senior managers. Weekly and monthly reconciliation records shall be compiled from the daily records. Reconciliation records shall be maintained for a minimum of one year. For Anti-Trust purposes, a review of records containing sales prices and cost information will not be included the APCP external audit.

11.9 Where applicable, the organization shall systematically consider the suitable and effective consideration and use of :

- a. Public key infrastructure (PKI);
- b. Certificate Authority (CA) authentication;
- c. Product key management and certificate lifecycle support PKI approaches through the process of creating, using and destroying public keys and digital certificates with which they are associated. The life cycle shall address controls for:
  - i. Key management
  - ii. Key generation (as created and held by the CA)
  - iii. Identity submission to the CA
  - iv. Registration of requests and its verification of submission identity
  - v. Digital certification
  - vi. Distribution of certificates
  - vii. Ensuring authorized usage
  - viii. Key & Certificate Renewal
  - ix. Recovery, when comprised
  - x. Proper Storage and archiving of certificates and their applications

---

## 12. ASSET HANDLING AND STORAGE

---

12.1 The organization shall identify all classes of assets and products to which these Standards and Procedures are applicable and the sites on which they are located, stored or processed. Assets may be in electronic or physical form. At a minimum, the list of assets and products shall include customer-supplied master data sources, finished products, and packaging materials designed to prove product legitimacy (e.g., hologram stickers and authenticity certificates).

12.2 All handling, processing and storage of the assets and products must be within the site's secure perimeter (see Section 10.1).

12.3 The site shall establish, implement and maintain procedures for logging and transferring assets and products throughout their possession from receipt to their eventual removal, destruction or return to the originator in accordance with Sections 12.9 through 12.13. The procedures shall be designed to allow effective tracking of assets as per Section 12.4

12.4 The site shall establish, implement and maintain procedures for tracking and counting (to a 1% degree of accuracy) assets and products in process. This will include the total number of content assets stored in digital format per content holder. Where tracking and counting identifies a discrepancy larger than 1%, reporting and investigation should be undertaken in accordance with section 12.7 of this Standard.

12.5 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. Frequency of the cycle shall be dependant upon the volume involved, but should be at least monthly.

12.6 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 secured perimeter.

12.7 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 raised and a management investigation 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.

12.8 Off site vendors and service providers must be vetted to ensure reliability and that reasonable security measures are in place, except when the client (as Risk Owner) requires a specific vendor or service provider or the organization is reasonably certain the vendor or service provider is reliable and has taken reasonable security measures (for example they are certified by CDSA in accordance with this Standard).

12.9 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.

12.10 Records must be kept of the return of all assets and products to clients or their designated agents.

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

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

12.13 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 organization is reasonably certain the courier is reliable and capable of tracking shipments.

12.14 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. It is recommended that such displays have the explicit approval of the product's owner.

12.15 The site shall establish procedures to document, authorize and correctly secure 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. Any security measures relating to assets or products removed from site shall conform to the spirit of the measures defined in this Standard.

12.16 The site shall implement back-up and restore procedures that satisfy not only contractual requirements but also the internal business requirement of the organization. These procedures must be in compliance with these Standards and Procedures, and back-up media shall be secured in a manner at least equivalent to the standard of the network from which it was taken.

12.17 The site shall document the number of network security incidents identified in the previous month, divided into minor/significant/serious categories, with trends analysis and narrative descriptions of all serious incidents and adverse trends. The analysis shall be conducted by appropriately qualified personnel under the scrutiny of the organization's risk management hierarchy.

12.18 The site shall implement procedures that provide protection against malicious and mobile codes on its network. These procedures must be in compliance with these Standards and Procedures.

---

### 13 PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

---

13.1 The organization shall establish, implement and maintain adequate and suitable measures to deal with disasters, unexpected events, and emergencies that would affect the confidentiality, integrity and availability of assets. A documented procedure(s) shall address:

- a. protections against damage from fire, flood, earthquake, and other forms of disasters,
- b. proper backup/restoration,
- c. the storage of records of preventive and corrective actions to maintain the integrity of systems, and
- d. the management of computer software security updates related to security threats, firewall/spyware/anti-virus approaches affecting a secure information systems environment.
- e.

---

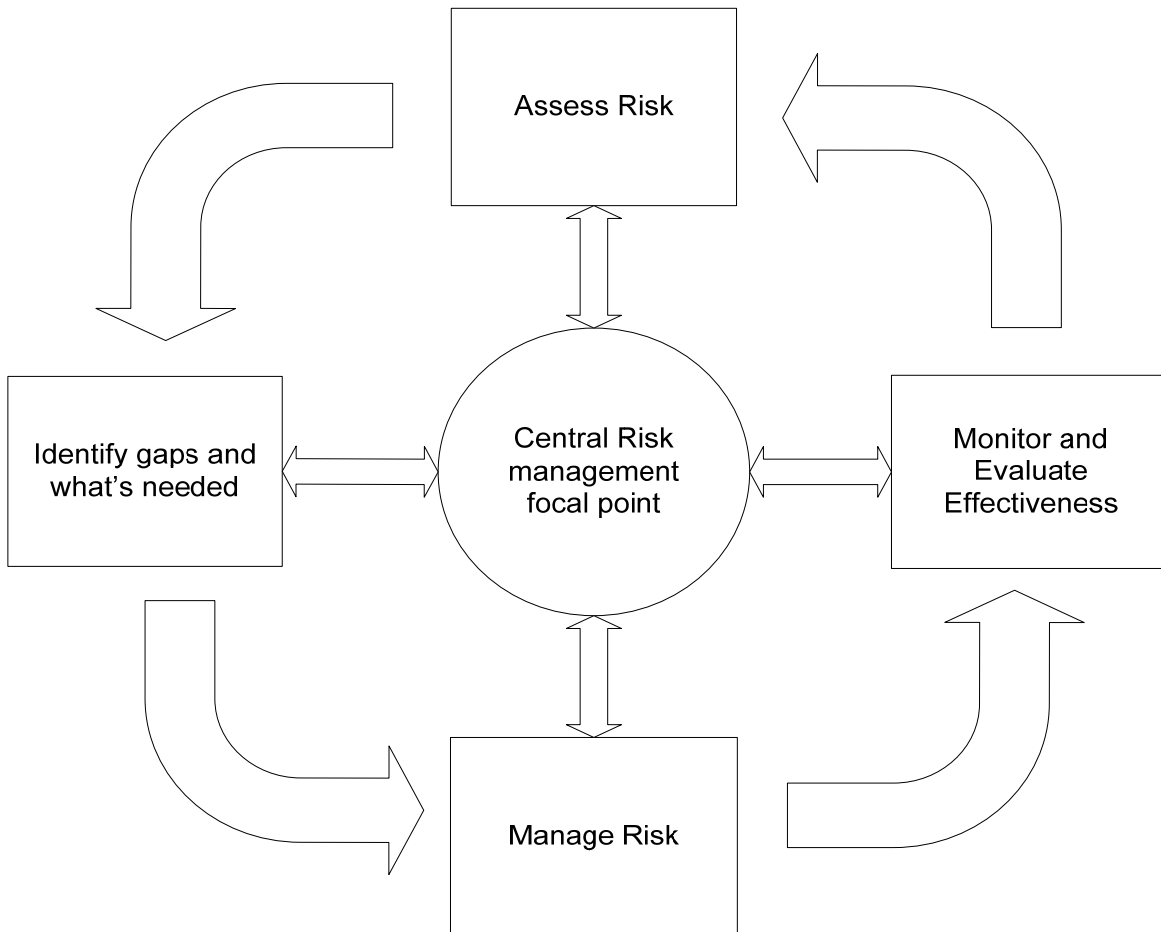
### DECLINATION OF LIABILITY

---

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.

## ADDENDUM 1

### RISK MANAGEMENT – ASSESSMENT – MITIGATION SYSTEM



1.1 The management of risk relies upon the correct identification of assets, assigning them an appropriate value, assessing the risks posed to them and devising a strategy to manage the risk. The process is continuous and cyclical since the threat environment moves constantly and therefore the nature of the risks will change with time.

1.2 Significant expense can be spent on the mitigation of risks, hence the importance of the assessment phase of the cycle. However, conversely significant unnecessary effort can be spared by the judicious use of sensible management strategies. There are 4 notional means of mitigating risks within the management cycle, and the selection of the correct one for each circumstance will deliver the best cost benefit, optimum performance and business output. While choosing an incorrect method will not necessarily result in an undue hampering of the business, it is unlikely to deliver value for money and an optimized business process.

1.3 Remember, risk ownership lies with the originating organization and is managed by those to whom it is delegated. The means of mitigating risk are commonly accepted as:

a. Remove. Removal of the risk is usually seen as an aversion strategy where it is unacceptable for taking of any degree of risk. Using this method, a risk of telephone conversions being intercepted would be managed by abandoning the making or receiving of telephone calls.

b. Reduce. A more conventional approach is the reduction of a particular risk to a level where the likelihood of its occurrence becomes more remote. The risk of a diamond being stolen is reduced by storing it in a safe; theft is still possible but less likely than leaving it on the dresser.

c. Transfer. A surprisingly widespread practice, the transference of financial risk is better known as insurance. In the context of the CDSA APCP: Content Protection and Security – Digital Download Supply Chain Standards and Procedures a record label transfers a portion of its risk to its supply chain partners. While ownership of the risk is maintained by the label, management of it is transferred to the supply chain.

d. Accept. Acceptance of risk is the last method and coincidentally usually occurs following the application of methods to reduce and transfer risks and/or the inability to remove them altogether. Where risk cannot be removed, reduced or transferred the only option is acceptance; in practice all reduction and transference will require some degree of acceptance, since there will be an element of risk remaining. This residual risk should be accepted at the appropriate management level based on impact the realization of the risk will have and the amount of budgetary leverage available to affect further mitigation.

1.4 For the purpose of demonstrating due diligence at a corporate level it is worth expending time and effort on clearly expressing and documenting the reasoning behind mitigation activities and articulating the resultant residual risks in terms that are meaningful to the business. This way the amount of residual risks being accepted on behalf of both the owner and the organization can be quantified and, if necessary, justified to shareholders and external auditors.

## ADDENDUM 2

---

### CONTENT SECURITY MANAGEMENT SYSTEM ELEMENTS

---

#### CONTENT SECURITY MANAGEMENT SYSTEM

---

i. The following information is provided as a guide for delineating the procedures and systems incorporated in an organization's operating manual for complying with the CDSA Anti-Piracy and Compliance Programs Content Protection and Security – Digital Download Supply Chain Standards and Procedures.

#### 1 SECURITY POLICY

---

1.1 Management should ensure that the security policy:

- a. is appropriate to the organization and its processes,
- b. demonstrates a commitment to meeting content security requirements,
- c. demonstrates a commitment to continual improvement of the content management system to meet customer requirements,
- d. is communicated and understood by personnel at appropriate levels of the organization, and
- e. is reviewed periodically to ensure revision as necessary.

1.2 The security policy shall be documented and controlled.

#### 2 ROLES AND RESPONSIBILITIES

---

2.1 The responsibility and authority of management involved in the security management system should be defined and documented, and clearly have support at board level. Documented procedures shall include management processes to:

- a. identify and ensure the availability of resources to demonstrate the organization's commitment to an effective security management system, including financial resources,
- b. identify training and competency needs of personnel and provide training to meet those needs. Records of training shall be documented and maintained,
- c. appoint a security management system program manager who shall ensure that the security management system, its policies and procedures are established, implemented and maintained in accordance with this Standard,
- d. promote and ensure communication and awareness of the content security management system processes and policies within the organization and between sites, where relevant, in a manner that encourages the involvement of personnel in achieving content security and continual improvement, and
- e. initiate audits, corrective actions, and preventive actions to minimize non-conformities relating to the Standard.

#### 3 DOCUMENT CONTROL

---

3.1 The organization should establish, implement and maintain documented procedure(s) to control documents that relate to the requirements of the Standard. The documented procedure(s) should identify methods and management authorization levels for:

- a. approval of documents for adequacy against the Standard prior to issue and distribution,
- b. ensuring changes and the current revision status are identified,
- c. reviewing and revising of documents as necessary,
- d. making document changes as a result of corrective action, preventive action, or other continual improvement of the content security system,
- e. ensuring documents remain legible and are easily identifiable,
- f. ensuring changes and the current revision status of documents are identified through suitable means such as a master list,
- g. accessing current versions of applicable documents at points of use,
- h. storing, maintaining and distributing documents as necessary, and
- i. preventing the unintentional use of obsolete documents by suitable means (if they are retained for any purpose).

3.2 Records shall be maintained to document conformance with the Standard and the specific requirements of the content security management system.

3.3 The organization should apply similar procedures to those listed at Section 3.1 of this Addendum in relation to its own internal documents where that documentation relates to the handling or protection of client-owned assets and products.

---

## 4 SITE EXIT AND ENTRY CONTROL

---

4.1 The organization should establish, implement and maintain procedures to control entry and exit points of its site to protect the confidentiality, integrity and security of customer intellectual property and related assets. To ensure the adequate and effective implementation of its control policies, the organization should document its procedures for:

- a. restricting and monitoring access to authorized individuals by suitable means,
- b. ensuring all unauthorized entrance and exiting from the site is prohibited using suitable methods,
- c. ensuring that all entry and exit points are monitored by suitable means during normal working hours,
- d. ensuring that all entry and exit points (e.g., entrance doors, emergency exits, windows, loading docks, etc.) are monitored and/or locked after normal working hours,
- e. Recording, electronically or manually, the time and date of entry and exits of all individuals entering or leaving the site for any reason (e.g., works breaks, meals, etc.), including company personnel and contractors. An exception may be provided for outdoor gathering points only if these areas are secured, monitored or manned in accordance with this Standard,
- f. Securing the site when it is unoccupied using reliable methods, including, at minimum, security locks on exit and entry doors and windows, and an alarm to detect unauthorized access to secure areas, and
- g. reporting to management any instances where entry control measures are believed to be inadequate, disregarded, or can otherwise be improved.

---

## 5 SITE SECURED AREA CONTROL

---

5.1 The organization should maintain procedures for controlling and monitoring access to internal areas containing content media or related assets, including vaults, safes, libraries and recording studios/control rooms. To ensure the effective implementation of its control policies, the organization should document its procedures for:

- a. controlling the area(s) where content media and/or related assets (e.g., tapes, discs, check discs, external removable hard drives and other media containing customer intellectual property) are stored,
- b. ensuring that entry and exit points to internal high risk area(s) are controlled and monitored,
- c. ensuring that access to the key, key card, or electronic access device is controlled by security personnel or other personnel authorized by management,
- d. restricting access to high risk area(s) to only a limited number of authorized individuals. These individuals should be monitored where feasible. The date and time of entry and egress, and reason for entry should be recorded by a means which can be available for later scrutiny if required, and
- e. using security devices (i.e., key-pad entry, intruder alert(s), alarms, etc.) to protect high security risk area(s) and detect unauthorized access. The use and location of security devices shall address, at minimum, coverage of building/site entrance(s) and exit(s), and sensitive areas (e.g., vaults, computer server, library, studio/control rooms, etc.).

---

## 6 CAMERA MONITORING AND MAINTENANCE

---

6.1 Where applicable law permits, the organization should monitor high security risk areas, including entry and exit points, shipping areas, content media and related asset production, storage and delivery area(s), and hallways, stairways, elevators, where appropriate, using CCTV. The quality of the images from the camera should be of a suitably high resolution to ensure that individuals can be identified from the footage in the monitored area(s).

6.2 The organization should establish, implement and maintain a documented camera preventive maintenance plan to ensure that security cameras are operated within specified parameters. Cameras should be fitted and maintained by a reputable supplier, who should have undertaken a pre-installation survey to ensure correct positioning, focal length and frame rate for the location of the camera. A frame rate of 3-5 frames per second is currently considered as the minimum acceptable rate. The preventive maintenance plan shall include methods for identifying, reporting and correcting camera failure, if it occurs.

---

## 7 CONTENT TRANSMISSION CONTROL AND MONITORING

---

7.1 The organization should establish, implement and maintain a policy and a documented procedure to control and monitor the content transmission and exchange by any means (e.g., email, FTP, whalemil, etc.). To ensure the effective implementation for its control and monitoring policies, the organization should document its procedures for:

- a. identifying the responsibilities of personnel authorized by management to receive, access or transfer/transmit customer content and related assets,
- b. determining policies governing any high risk media devices (e.g., PDAs, cellular camera telephones, digital cameras, compact/removable discs, flash drives and recordable disc drives, etc.),
- c. preventing, restricting and monitoring email transmission, internet, and FTP transmission to authorized recipients to ensure their use for valid business purpose(s) only,
- d. limiting and controlling access to computer workstations to only authorized users, including procedures for log-in, identification and authentication of all users, dedicated user accounts, and password maintenance and management,
- e. identifying a computer workstation administrator with the sole authority to manage user accounts, modify or configure hardware or software applications and allocate access rights and user registration,
- f. implementing terminal controls, including computer logs to record critical events and monitoring workstation activities,
- g. isolating sensitive data (such as digital content) from Information Technology processing systems and internal/external networks used for business tasks (e.g., non-production activities, such as word processing, email, efax, and intranet, and internet access, etc.) from workstations used to manipulate and store content and related assets,
- h. Protecting the organization's local and wide area networks (Including WiFi networks), and
- i. logging transmission of all sensitive content and related assets transferred and/or transported in or out of the site.

---

## 8 CONTENT ACCESS CONTROL AND MONITORING

---

8.1 The organization should maintain procedures for controlling and monitoring access to all internal, high security risk area(s) containing customer intellectual property, including vaults, safes, libraries and recording studio(s)/control room(s). Management shall establish, implement and maintain documented procedure(s) that include methods to:

- a. identify and provide high security area(s) for the storage of media such as tapes, discs, check disc, external removable hard drives and other media containing customer intellectual property. The same security standard should be used to protect incoming media downloaded into the site's production and/or storage systems,
- b. ensure that access points to high security risk area(s) are monitored and assessed to verify that they remain locked at all times. These access points should be restricted to authorized individuals only. All unauthorized entry/egress to and from these areas should be reported,
- c. ensure that security devices, such as electronic keys, are controlled by suitable means,
- d. restrict access to high security risks area(s) to authorized individuals only,
- e. secure high risk security area(s) after normal business hours or when they are unoccupied,
- f. define and enforce appropriate access control for all cleaning and maintenance personnel, including after hours access, and
- g. define and restrict remote access to internal computers and equipment that store or process sensitive data.

---

## 9 MEDIA ACCESS CONTROL AND MONITORING

---

9.1 The organization should establish, implement and maintain documented procedure(s) for controlling and monitoring the receipt, internal use, transfer and/or destruction of content media and related assets containing intellectual property. To ensure the effective implementation of its control and monitoring policies, the organization should document its procedures for:

- a. ensuring content traceability methods. Traceability methods shall address the chain of custody, including the recipient(s) of content media assets,
- b. Logging of on-site media transactions, and
- c. identifying customer intellectual property, content media and related assets in respect of destruction / scrapping processes, including record maintenance and retention methods, and those authorized to perform such processes.

---

## 10 DEVICE CONTROL AND MONITORING

---

10.1 The organization should establish, implement and maintain policies for authorizing, managing and monitoring the internal use and processing of content media devices (e.g., laptops, PDAs, removable media devices, temporary storage devices, portable hard drives, memory sticks, cell phones, USB storage devices, MP2 players, permanent storage devices, including devices used for file back-up). The organization shall document procedure(s) to identify content media devices used, and their authorized use(s) under controlled conditions, including:

- a. determining the need for individuals to use such devices,
- b. registering devices and individuals authorized to use them,
- c. restricting and monitoring the use of approved portable storage devices. All such devices should be labeled with a unique identifier, audited, and accounted for on a regular basis,
- d. periodic audits and/or verification of the continuing need for each authorized user to have access to such devices, and
- e. methods for restricting and disabling unauthorized devices, peripherals or ports on the organization's computer equipment (including servers, FTP sites and other file transfer servers).