Content Delivery & Security Association

Content Protection & Security Standard

DOCUMENTATION, RISK MANAGEMENT AND COMPLIANCE

PERSONNEL AND RESOURCES

ASSET MANAGEMENT

PHYSICAL SECURITY

IT SECURITY

TRAINING AND AWARENESS

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Content Protection & Security Program

Revised January 31, 2013

About this Standard

The goal of the CPS Standard is to secure media assets at all stages of the supply chain. This objective-based approach establishes seven frameworks of capability.

- **Content Protection and Security Standard**
  - **CF 1: Documentation, Risk Management and Compliance**
  - **CF 2: Personnel and Resources**
  - **CF 3: Asset Management**
  - **CF 4: Physical Security**
  - **CF 5: IT Security**
  - **CF 6: Training and Awareness**
  - **CF 7: Business Continuity and Disaster Recovery Planning**

The requirements defined within the Standard and its accompanying guidance form the basis of a Content Security Management System (CSMS). This consists of cohesive policies, processes and controls that are designed to assess, manage and minimize risks to an acceptable level, thereby ensuring the continued integrity of intellectual property, confidentiality and media asset security.

In determining content protection requirements, CDSA have assessed industry specific risks, identified threats and current vulnerabilities that are encountered within the industry. This process has facilitated the formulation of a suite of objectives to control and/or mitigate those risks, threats and vulnerabilities.

These objectives provide the basis on which to define the auditable requirements for certification with the CDSA Content Protection and Security (CPS) program.

The Audit Process

Once a site has applied for the Program, CDSA provides it with this document and a Statement of Applicability (see below). A timeframe for the initial audit is then set following which a detailed report will be submitted to the site. A further Audit is undertaken six months later, and thereafter audits follow every 12 months.

A site is evaluated against the requirements of this Standard, within the scope of the audit set by the Statement of Applicability. This takes place during an on-site visit by a qualified CDSA auditor.

The site receives certification if:

- there are zero non-compliances, or
- one or more non-systemic (minor) non-compliances need to be addressed by an agreed corrective action plan and no significant threat to client media assets is identified.

Facilities where one or more major or systemic non-compliances are observed fail to achieve certification until the issues are adequately addressed, and have been re-evaluated and accepted by CDSA.

A major non-compliance occurs where a significant threat to client media assets is identified and may include:

- a failure to meet a critical individual requirement, or
- an objective not being met as a result of systematic failure to meet the Standard.

How to use this Standard

In order to remain applicable to a wide cross-section of participants from the supply chain industry, this document remains vendor and technology neutral. Inconsistent usage or conflicting usage of terminology is a major hindrance to effective communication, so to avoid confusion, this Standard utilizes the following terms:

- **Content Protection Security:** The preservation of confidential intellectual property and protection of media related assets, against all threats, whether internal or external, accidental or deliberate.
- **Policy:** WHAT to do
- **Process or Procedure:** HOW to do it
- **Role:** WHO is responsible and corresponding competencies
- **Responsibility:** What task/s an individual is accountable for in accordance with any policy or procedure
- **Schedule:** WHEN an action is performed

The participant of the program is referred to as ‘site’ notwithstanding that in many instances a site is part of a larger organization.

All requirements in this Standard are addressed in a documented entitled “Statement of Applicability” (SoA). A template SoA is available from CDSA.

- Requirements deemed **Not Applicable** must be identified and justified.
- Requirements deemed **Applicable But Not Implemented** must be identified and justified, for example:
    - In progress
    - Future project
    - Accepted risk
- Requirements **Not Addressed As Described In This Standard** may be justified through detailing equivalent compensating controls that meet the same objective.

Each capability framework includes the following sections:

Objective: A measureable objective paired with a series of auditable requirements to be addressed.

Requirements: High-level description of the requirement(s) to be met.

Compliance Mapping: Reference to industry best practice such as ISO and MPAA.

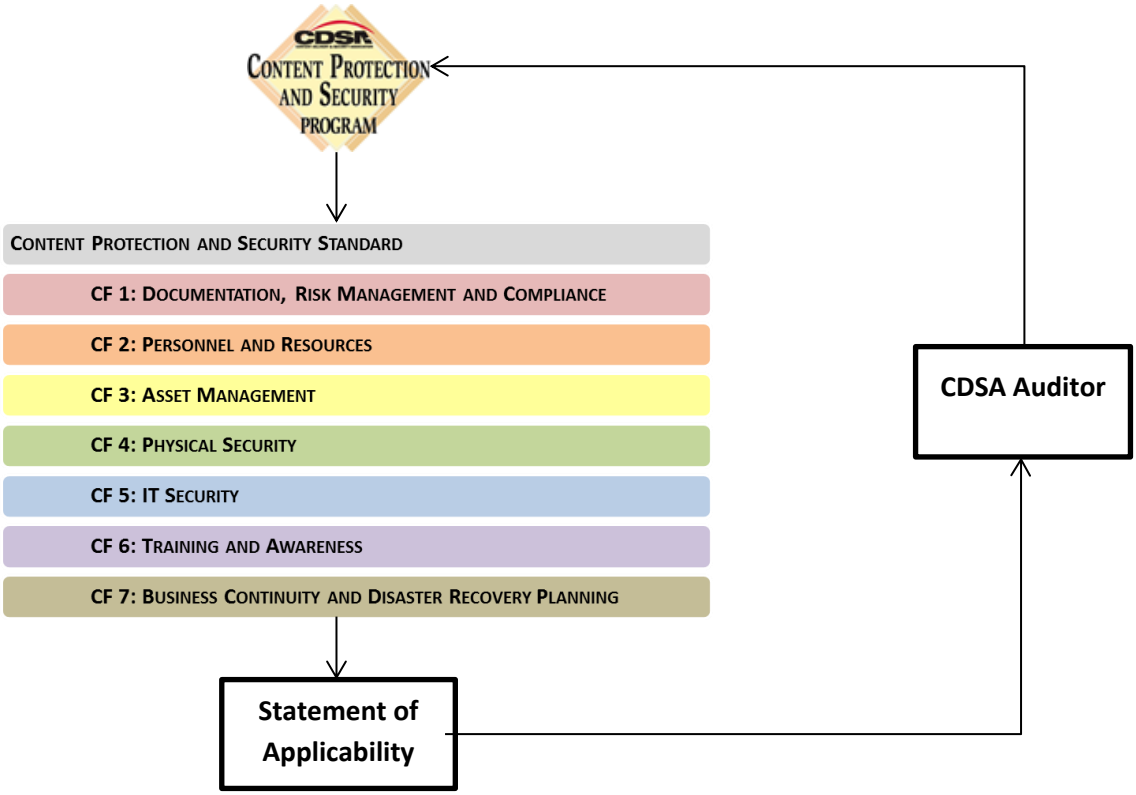
Further guidance is available through consultation with the appointed auditor or territory director.

The Statement of Applicability

Certification to this Standard begins with the site completing an internal assessment against the CPS Standard requirements. This is followed by the completion of a "Statement of Applicability" or SoA.

In completing the SoA, the site evaluates all requirements as detailed in the Standard, noting what requirements are applicable and finally what has been done to meet the requirement. A completed SoA is imperative because:

- It can be utilized by a site to determine readiness for CDSA evaluation,
- It can be utilized by a site to document and demonstrate equivalent methods by which an objective is met, but may be divergent from the defined requirements,
- It can be utilized by a site to document those requirements identified as not applicable within the environment under consideration, and
- It is used by the CDSA auditor to set the scope of the audit, including appropriate resources and duration.



Declination of Liability

CDSA has made every effort to formulate a Standard that it believes helps sites reduce the likelihood of content loss or theft. However, a Standard, no matter its specificity or diligent application, cannot guarantee avoidance of a loss or claim. Therefore, CDSA is not liable for any loss or claim by a content owner, site or organization, or other party on account of this Standard, whether or not CDSA has issued a certificate of compliance.

CF 1. DOCUMENTATION, RISK MANAGEMENT AND COMPLIANCE

CF 1.1. Documentation

Objectives: Design and produce a security policy manual and associated documentation.
Communicate all security policies, procedures and work instructions to staff.
Ensure documents remain current and fit for purpose through a process of review.

Requirements:

CF 1.1.1. The site shall establish, implement and maintain a process to control documents and records that relate to its security management system. This process shall include methods for:

- approving documents prior to use,
- ensuring that document changes and current revisions are properly identified through an appropriate means,
- reviewing and updating documents when needed,
- ensuring documents are legible, identifiable, properly stored and maintained,
- ensuring current documents are available where needed, and
- preventing unintended use of obsolete documents.

All such records and documentation shall be retained for a minimum of 3 years, except where specified otherwise.

CF 1.1.2. The site shall establish, implement and maintain a content protection and security policy manual to document its systems, procedures, processes, policies, responsibilities and authorities, and its conformity to requirements.

CF 1.1.3. The control documents shall specify operational procedures necessary for conformity.

CF 1.2.	Risk Management
Objectives:	Conduct a review of the entire business activity in each department and identify all potential security related risks. Implement proportionate and effective controls to prioritize and mitigate identified risks. Manage and review risks within a process of continual review.
Requirements:	
CF 1.2.1.	Management shall define roles and responsibilities for risk assessment.
CF 1.2.2.	The site shall document a Statement of Applicability that summarizes the capabilities that shall be implemented and any exclusion from the CPS security requirements.
CF 1.2.3.	Risk assessments shall be documented, describing each risk, analyzing its level of importance and assessing the likelihood of an un-controlled event occurring.
CF 1.2.4.	The method for identifying and prioritizing risks shall be provided.
CF 1.2.5.	A risk treatment plan shall be documented to identify the method by which the site has treated the risk.
CF 1.2.6.	Risk assessments shall be recorded, reviewed and agreed by senior management annually and/or when changes in business activity occur.

CF 1.3. Compliance

Objectives: To ensure the site has considered applicability to the CPS Standard, legal, regulatory and contractual obligations.
To provide a mechanism to promote on-going compliance.

Requirements:

CF 1.3.1. Management shall define and implement procedures for evaluating site compliance to security management system requirements. Evaluation methods shall include processes for:

- security incident monitoring and response,
- corrective and preventive actions,
- internal audits,
- external CDSA audits, and
- management review of security management system performance.

CF 1.3.2. The site shall establish, implement and maintain a process for security incident monitoring and response. Procedures shall address methods for:

- identifying the type of security incident (e.g., previously unidentified risk, failure to follow security procedures, security hardware failures, theft or loss of intellectual property or related media assets, or any other unusual situation possibly affecting security),
- gathering details and where necessary securing evidence of the security incident (e.g., date, time and location of incident, circumstances, persons involved, etc., and considering the need for specialist resources for incident handling and evidence gathering),
- investigating security incidents and their root causes,
- evaluating the significance and impact of the actual or potential loss,
- initiating immediate response and recovery plans to mitigate loss and prevent ongoing risk where necessary, and
- escalation procedures for investigation including client notification and regular updates.

CF 1.3.3. Corrective and preventive action processes shall:

- eliminate the root causes and prevent reoccurrence,
- eliminate any potential for unauthorized release or access to content and prevent reoccurrence,
- ensure timely and effective response,
- measure responses to ensure they remain proportionate to the risk, and
- address any non-compliance as a result of an incident or as a result of internal and external audit results.

The site shall maintain and retain associated records for at least three years.

CF 1.3. Compliance

CF 1.3.4. Internal audit procedures shall ensure:

- operations comply with the CPS Standard and any legal, regulatory or contractual obligations,
- security controls implemented provide sufficient protection to assets and that they are adequately maintained,
- internal audits are scheduled and performed at least once per year,
- where practicable persons carrying out the audit shall be independent of those having direct responsibility for the activity,
- results of the audits are recorded and published to enable those responsible to make corrective or preventive action,
- review processes verify timely completion and record the implementation and effectiveness of corrective actions, and
- results of internal audits and corrective actions are included in management reviews.

CF 1.3.5. External audit shall be conducted according to the following:

- management shall review the performance against the CPS requirements at specified intervals to ensure its continuing suitability and effectiveness; as a minimum one annual internal audit shall be completed no later than six months following the CDSA 6 month external audit,
- on successful completion of an initial external CPS audit the site shall be certified for a six-month period,
- following the initial six-month certification period a further external CPS audit shall be carried out and, if successful, the site shall be certified for a 12-month period,
- the site shall then undergo external CPS audits on an annual basis,
- certification periods run to the end of the month in which the audit was due,
- delayed audits are backdated,
- audits can be brought forward no more than one calendar month, and
- audits delayed longer than three months result in removal from the certification process.

CF 1.3.6. Non-compliances detected during external audits are defined and managed as follows:

- a major non-compliance occurs when there is evidence that assets are placed at significant or long-term risk,
- additionally, a major non-compliance occurs when it is identified that there is a systemic failure to meet the requirements of the CPS program,
- where major non-compliances are found, the site shall not receive certification until it implements effective corrective actions and these have been thoroughly verified, possibly through a re-audit (all cases of systemic failure require a re-audit),
- a minor non-compliance is a non-systemic, non-fulfillment of an element of a clause of the requirements of the CPS program,
- where minor non-compliances are found the site shall have 30 days to submit a corrective action plan to the CDSA auditor,
- once the plan is agreed CDSA issues a certificate of compliance,
- CDSA reserves the right to suspend certification until appropriate corrective actions are implemented, and

CF 1.3. Compliance

- CDSA reserves the right to publicly acknowledge certification suspension.

CF 2. PERSONNEL AND RESOURCES

CF 2.1. Personnel and Resources

Objectives: Mitigate the risk to content where personnel and resources are involved, including the engagement of contractors, consultants and third-party vendors.
Provide adequate budget to support security objectives

Requirements:

CF 2.1.1. Management shall appoint a CPS program manager who shall ensure that the security management system, its policies and procedures are established, implemented and maintained.

CF 2.1.2. Management shall define its organizational structure.

CF 2.1.3. Management shall assign roles and responsibilities to process owners, who effectively develop, implement and maintain security policies and procedures to secure assets and meet security objectives. The responsibilities and authorities of management involved in the security management system shall be defined and documented.

The organization shall have policies for:

- recruiting and hiring practices,
- new hire background screening and review,
- confidentiality agreements,
- job changes and reassignments,
- disciplinary actions against personnel, and
- personnel termination practices.

CF 2.1.4. Management shall take appropriate action to make arrangements for job changes, reassignments, and personnel terminations, including:

- asset and knowledge transfer and
- reassignment and/or removal of access rights.

CF 2.1.5. Management shall ensure that areas of responsibility are separated where necessary to reduce opportunities for unauthorized modification and misuse of information or services.

CF 2.1.6. Management shall identify and ensure the availability of adequate budget for mandated security requirements.

CF 2.1.7. Management shall identify any other resources (other than financial) that may be of benefit to the security management system and/or managing security risks.

CF 2.1.	Personnel and Resources
CF 2.1.8.	Management shall ensure that appropriate Service Level Agreements (SLAs) and contractual obligations are agreed, implemented and reviewed regularly.

CF 2.2.	Third-party Resources
Objectives:	Minimize the risk to assets entrusted to, under control of or accessed by contractors, consultants and third-party vendors
Requirements:	
CF 2.2.1.	The site shall have policies and procedures for the contracting and engagement of any third-party resources. Policy and processes for third-parties shall conform to relevant CDSA requirements. As a minimum this shall include: • background screening and due diligence, • third-party recruitment hiring and termination, • third-party insurance consistent with that of the site, • confidentiality and non-disclosure agreements, • documented supplier risk assessment, • acceptance of independent audit/review, and • documented annually performed internal audit. Documents shall be retained for a period of three years.

CF 3. ASSET MANAGEMENT

CF 3.1. Administrative Controls

Objectives: Ensure that roles and responsibilities for asset management and security are established and have been clearly communicated.
Ensure a consistent approach when handling assets using a process of risk assessment.
Provide a secure, efficient and effective operating system for all assets.
Ensure additional security requirements are considered, authorized and implemented.
Maintain documented policy and process for digital IP and other commercial assets.

Requirements:

CF 3.1.1. Management shall define specific roles and the responsibilities for each stage of asset handling. This may include:

- receipt and identification of incoming assets,
- asset identification and traceability,
- asset handling,
- asset storage, and
- transport of outgoing assets.

Such policies shall ensure the security of physical assets,analog and digital recordings, removable drives, including reference copies, temporary storage devices for digital files and permanent storage devices including backups of content.

CF 3.1.2. Personnel shall acknowledge an understanding and acceptance of their specific role.

CF 3.1.3. Management shall assign a risk category for each asset based on type of content being handled, i.e., high value, pre-release, back catalog, etc.

CF 3.1.4. Each risk category shall have assigned specific security requirements.

CF 3.1.5. Each asset handling procedure shall be documented to ensure a consistent approach.

CF 3.1.6. Access to computer systems and storage locations for digital assets shall be properly administered to prevent unauthorized access.

CF 3.1.7. Access to asset locations shall be reviewed regularly.

CF 3.1.8. Documents shall be retained for a minimum of three years.

CF 3.2.	Control of Assets
Objectives:	Implement, operate and maintain an accurate asset management system that is capable of audit.
Requirements:	
CF 3.2.1.	The site shall introduce an asset management system. The system may be electronic or paper-based.
CF 3.2.2.	The system shall be capable of providing an auditable chain of custody, identifying the location and time/date of creation, movement or destruction.
CF 3.2.3.	Records shall be retained for a minimum period of three years.

CF 3.3.	Asset Receipt and Identification
Objectives:	Implement, operate and maintain accurate records for asset receipt and future identification.
Requirements:	
CF 3.3.1.	Document a process for recording unique reference identification for assets at the point of receipt.
CF 3.3.2.	All assets shall be uniquely identified and logged in upon arrival. This can include use of bar code or other unique identification.

CF 3.4.	Asset Handling and Transfer
Objectives:	Implement, operate and maintain an effective process for asset tracking. Maintain accurate records of all asset movement that are capable of audit.
Requirements:	
CF 3.4.1.	Document an asset transfer process that demonstrates how assets are transferred and traced on-site and, where applicable, off-site at third-party vendor locations.
CF 3.4.2.	Document an asset handling process that details the security requirements necessary to ensure the integrity and security of assets.
CF 3.4.3.	Ensure all asset movement is logged, audited and reviewed throughout the assets' chain of custody.

CF 3.5.	Secure Asset Storage and Reconciliation Controls
Objectives:	Maintain accurate records for asset storage and movement. Ensure asset integrity and security is being maintained.
Requirements:	
CF 3.5.1.	The site shall allocate assets to secure locations identified within the site security plan.
CF 3.5.2.	Locations shall be subject to enhanced security controls to ensure access is only permissible to authorized personnel.
CF 3.5.3.	The site shall establish and implement a cyclic count policy for stored assets.
CF 3.5.4.	Where possible, personnel independent of the asset management process shall carry out cyclic counts.
CF 3.5.5.	Management shall periodically review cyclic counts procedures and results.
CF 3.5.6.	Discrepancies shall be investigated and reviewed by management.
CF 3.5.7.	A process for client notification and escalation shall be documented.

CF 3.6.	Asset Re-call Procedures
Objectives:	Prevent assets from being retained outside secure storage locations any longer than is necessary. Reduce opportunity for theft and prevent assets from being left unattended. Provide a mechanism whereby escalation procedures can be implemented, including commencement of checks, controls, investigation and client notification.
Requirements:	
CF 3.6.1.	The site shall adopt a procedure for asset recall, identifying criteria for items according to risk assessment.
CF 3.6.2.	Where an asset cannot be accounted for, a person responsible for the activity shall conduct an initial investigation to recover the item.
CF 3.6.3.	The results of any investigation shall be documented and reported to line management. Rectification, corrective or disciplinary action shall be considered to avoid future incidents.
CF 3.6.4.	Should an asset remain missing beyond an initial investigation, further inquiry shall be commenced using a person independent of the activity.
CF 3.6.5.	A policy and procedure for escalation and client notification shall be in place. Policy and procedures must be compliant with any service level agreement or contractual requirement.

CF 3.7.	Control of Blank Media Materials
Objectives:	Treat raw materials as an asset. Document, implement and maintain secure processes for controlling raw material.
Requirements:	
CF 3.7.1.	Document an asset identification process for all raw media arriving on site.
CF 3.7.2.	Ensure all blank/raw media is and logged in upon arrival. Whenever possible, the blank raw media shall be uniquely identified. This can be either by use of barcode or another unique identifier.
CF 3.7.3.	Ensure all raw media is stored in a secure location and access restricted to authorized personnel.
CF 3.7.4.	Document an authorization and tracking process for signing out all raw media for use.

CF 3.8.	Record Retention
Objectives:	Retain accurate and detailed asset management records to enable and assist audit and investigation.
Requirements:	
CF 3.8.1.	The site shall establish a policy and procedure for record retention. As a minimum, this shall include all asset receipt/dispatch records, manufacturing process documentation and asset tracking records.
CF 3.8.2.	The site shall ensure that all records are retained for a minimum period of three years.
CF 3.8.3.	Where samples are retained for quality purposes or in compliance with other certification programs; these shall also be retained for a minimum period of three years.

CF 3.9.	Transportation of Assets
Objectives:	Achieve secure transfer of assets between sites.
Requirements:	
CF 3.9.1.	The site shall establish policy and procedures for the secure transportation of assets.
CF 3.9.2.	Assets must be prevented from leaving a site until all checks and authorities for shipment have been met.
CF 3.9.3.	Policy and procedures shall set out a minimum security standard for vehicles and driver conduct.
CF 3.9.4.	Policy and procedures shall determine when and how vehicles shall be sealed prior to shipping, according to documented risk assessment and client contractual obligations.
CF 3.9.5.	For high profile loads, requirements for additional guarding and vehicle tracking shall be considered as part of a documented risk assessment.
CF 3.9.6.	Driver policy and procedure shall prevent unsecure and unattended parking.
CF 3.9.7.	Third-party couriers or haulers shall be subject to a written Service Level Agreement and carry sufficient liability insurance to cover client losses in the event of the theft or loss of a high profile release.
CF 3.9.8.	There shall be a documented policy that ensures visiting drivers do not enter the premises, or, where necessary, are escorted at all times.

CF 3.10.	Labeling and Packaging
Objectives:	Achieve secure transfer of assets between sites.
Requirements:	
CF 3.10.1.	The site shall implement and maintain a documented policy and procedures for the labeling and packaging of all assets leaving the site. Client specific requirements must be taken into consideration.
CF 3.10.2.	Inconsistent, differentiating use of packaging and title-based identification shall be avoided. Where possible, details shall be restricted to order number, unique reference numbering, quantity and destination.

CF 3.11.	Destruction and Recycling
Objectives:	Secure assets in segregated containers and monitor locations while awaiting destruction. Securely destroy and recycle assets using a reliable and auditable process.
Requirements:	
CF 3.11.1.	The site shall implement and maintain documented policy and procedures for destruction and recycling.
CF 3.11.2.	Processes shall ensure that assets are rendered unusable and/or securely stored within suitable locked containers while in production and manufacturing environments. Containers shall be transferred for destruction on a frequent basis. The long-term retention of assets awaiting destruction must be avoided.
CF 3.11.3.	While awaiting secure destruction, assets must be securely stored and monitored.
CF 3.11.4.	In the case of optical disc manufacturing, molded reject discs used in print set-up processes must be rendered unusable by a client-approved method.
CF 3.11.5.	Storage containers for rejected items awaiting destruction shall be clearly marked to avoid mistaken identity.
CF 3.11.6.	Detailed records shall be maintained for all assets destroyed, detailing the number, weight, date and time of destruction. A certificate of destruction must be made available for clients wishing formal conformation. Records must be retained for a minimum of three years.
CF 3.11.7.	Where on-site grinders are used, they shall be monitored by CCTV.
CF 3.11.8.	Where destruction or recycling is performed by third-parties, a Service Level Agreement must be in place ensuring the above requirements are met.
CF 3.11.9.	Third-parties shall provide certificates of destruction to confirm that all assets have been destroyed in accordance the above requirements.

CF 4. PHYSICAL SECURITY

CF 4.1. Physical Security Management

Objectives: Document within a security plan what physical security controls are in place and how these are monitored to safeguard designated critical, sensitive and operational assets.
Demonstrate within a security plan how unauthorized physical access to perimeter and internal secure areas are prevented, monitored and managed.
Demonstrate within a security plan how physical access to perimeter and internal secure areas is authorized, monitored and managed.
Demonstrate within a security plan how physical access controls protect specific locations where assets and critical business information is located.

Requirements:

CF 4.1.1. The site shall establish a physical security plan.

CF 4.1.2. The plan shall demonstrate that risks to personnel, media assets and business continuity have been properly considered and that controls are in place to reduce risks to an acceptable level.

CF 4.1.3. As a minimum, the plan shall provide policy and procedures for:

- site access, authorization and denial to include pedestrians and vehicles, visitors, contractors and employees,
- segregation of all operational areas where assets, including blank material, are received, handled, manufactured, stored and dispatched,
- site monitoring and patrol,
- incident prevention, detection and response, and
- security breaches and unauthorized access specifically relating to the integrity of media assets.

CF 4.1.4. The plan shall consider the security controls needed to mitigate environmental risks as part of risk assessment.

CF 4.2.	Perimeter Security
Objectives:	Physically secure the site perimeter using appropriate, proportionate and effective controls and boundaries.
Requirements:	
CF 4.2.1.	The site shall detail policies and procedures for controlling the site perimeter within a site security plan.
CF 4.2.2.	The site shall demonstrate its capability to secure the physical perimeter. The site shall be protected by a continuous physical barrier that is inspected and reviewed regularly.
CF 4.2.3.	All entry and exit points shall be secured and monitored using appropriate means to ensure the integrity of the physical boundary and protection of assets.

CF 4.3.	Securing Internal Areas
Objectives:	Ensure the internal security of a site, and identify requirements for high security zones. Monitor, secure and control access to internal areas where media assets are located, stored, handled or produced.
Requirements:	
CF 4.3.1.	The site shall implement and maintain policies and procedures for accessing, monitoring and controlling internal locations and secure areas.
CF 4.3.2.	The site shall provide clear delineation of controlled and secure areas.
CF 4.3.3.	Creation of each zone shall be risk assessed against the activity being undertaken, media asset value, perceived threats or vulnerabilities and environmental protection.
CF 4.3.4.	The site shall control access to buildings. Internal areas containing media assets shall be segregated, secured and monitored to prevent unauthorized access.
CF 4.3.5.	Segregated secure areas must be subject to access control and monitoring.
CF 4.3.6.	The level of physical controls required shall be risk assessed against the activity being undertaken, media asset value, perceived threats or vulnerabilities and environmental protection.
CF 4.3.7.	Access to assets shall only be permitted where there is a legitimate business need.
CF 4.3.8.	Sites shall ensure that security controls provide prevention, detection and responses to security incidents.
CF 4.3.9.	Authorized access to secure internal areas for personnel shall be established according to their roles and responsibilities.
CF 4.3.10.	The possession and use of personal photographic, recording, storage and audio devices shall be controlled or prohibited when operating or visiting secure internal areas.
CF 4.3.11.	The site shall implement and maintain policies and procedures for visitor access. To include details of registration, search policy and escorted access to secure locations.

CF 4.4.	Use of Guards
Objectives:	Ensure the integrity and security of the physical site by the use of guards.
Requirements:	
CF 4.4.1.	The site shall implement and maintain policies and procedures of guarding duties including the creation, management and audit of site assignment instructions.
CF 4.4.2.	The site shall establish effective processes to deal with perceived threats, including response and reporting plans.
CF 4.4.3.	Where third-parties are used, requirements set out in CF 2 shall be followed.

CF 4.5.	Searches
Objectives:	Deter and detect the theft or misappropriation of assets.
Requirements:	
CF 4.5.1.	The site shall implement and maintain policies and procedures for searching that include all persons leaving a designated secure area.
CF 4.5.2.	A process for escalating a positive search and recording search details shall be adopted.
CF 4.5.3.	Searches shall be both random and for cause with a recommended minimum of 20 percent of egress numbers being subjected to the search criteria.
CF 4.5.4.	The extent of searches shall be limited to legal and regulatory controls, but where possible must include the removal of outer wear, the emptying of pockets, bag inspection, and the use of a hand held metallic detector.
CF 4.5.5.	Searches of vehicles shall be implemented where personal vehicles are allowed within controlled and secured areas as defined in CF 4.3.
CF 4.5.6.	A record of searches shall be retained for a minimum period of 90 days.

CF 4.6.	CCTV
Objectives:	Protect premises, staff and media assets through the effective use of CCTV.
Requirements:	
CF 4.6.1.	Where CCTV is used appropriate policy shall be established and communicated.
CF 4.6.2.	Images are to be secured for a minimum of 90 days and only accessed by persons with legitimate business need.
CF 4.6.3.	Images shall be time and date stamped.
CF 4.6.4.	Monitoring shall be carried out using suitably qualified staff. Irrespective of deployment, sites shall consider local laws and regulation of deployed CCTV.
CF 4.6.5.	There shall be suitable maintenance agreement or suitable internal arrangements in place.
CF 4.6.6.	Systems shall be maintained in accordance with manufacturer's guidelines. Where third parties are used, requirements set out in CF 2 shall be followed.
CF 4.6.7.	Uninterrupted power supply (UPS) must extend to all security systems and sized appropriately for local conditions and business activities.
CF 4.6.8.	Adequate lighting shall be maintained to ensure clarity of vision and recordings.

CF 4.7.	Access Control Systems and Automated Technologies (AACS)
Objectives:	Protect external and internal access to controlled and designated internal secure areas through the use of automated access control systems.
Requirements:	
CF 4.7.1.	The site shall implement and maintain policies for use in monitoring and controlling access control systems. The policy shall address shall address situations of system failure, tampering or avoidance.
CF 4.7.2.	Events and movements to sensitive areas shall be logged, available for immediate review, and retained for a minimum of three years.
CF 4.7.3.	Systems shall be maintained in accordance with manufactures guidelines. Where third party services are used requirements set out in CF 2 shall be followed.

CF 4.8.	Intruder Detection Systems (IDS)
Objectives:	Detect the entry, or attempted entry of an intruder into a protected area. Identify the location of the intrusion and to signal an alarm on which to respond.
Requirements:	
CF 4.8.1.	The site shall implement and maintain policies for using and monitoring and controlling IDS.
CF 4.8.2.	Where installed sites shall ensure that systems are maintained and routinely tested.
CF 4.8.3.	If maintained and tested by a third-party the site shall operate a service level agreement to ensure constant coverage.
CF 4.8.4.	Access to the system shall be controlled in accordance with IT Security CF 5 requirements.
CF 4.8.5.	The IDS shall have uninterrupted power supply.
CF 4.8.6.	The IDS shall be monitored and responded to when activated.
CF 4.8.7.	Event logs for the preceding 90 days shall be available for review.

CF 5.	IT SECURITY
CF 5.1.	**Information Security Management**
Objectives:	Establish a document framework for IT controls.
Requirements:	
CF 5.1.1.	IT security policy shall be defined and published.
CF 5.1.2.	Reference shall be made to the technical controls and practices employed to secure the enterprise information systems.
CF 5.1.3.	IT security policy shall be agreed by management and subject to regular review.
CF 5.1.4.	IT security policy shall define principles, standards and compliance requirements.

CF 5.2.	Acceptable Use
Objectives:	Provide a formal framework for acceptable system, network, and asset usage. Achieve a culture of responsible behavior at all levels of the organization when working with client assets.
Requirements:	
CF 5.2.1.	The site shall establish, implement and maintain an acceptable use policy for acceptable use of IT assets.
CF 5.2.2.	The policy shall define rules pertaining to acceptable use and responsibilities of all users irrespective of association, i.e., employee, contractor, temporary staff, consultants and visitors.
CF 5.2.3.	The policy shall define the disciplinary consequences of non-adherence to the acceptable use policy.
CF 5.2.4.	The policy shall be communicated and a record maintained of the individual's understanding and acceptance of the content.

CF 5.3.	Internet Usage
Objectives:	Provide a formal framework for acceptable Internet usage. Achieve a culture of responsible Internet usage at all levels of the organization.
Requirements:	
CF 5.3.1.	The site shall establish, implement and maintain an internet acceptable use policy.
CF 5.3.2.	The policy shall include: • individual responsibilities and accountability, • what constitutes acceptable and unacceptable behavior • actions required should inappropriate internet access or use be suspected, • consequences of unacceptable Internet use, and • training and awareness requirements.
CF 5.3.3.	The policy shall be communicated and a record maintained of the individual's understanding and acceptance of the content.

CF 5.4.	E-mail Usage
Objectives:	Provide a formal framework for acceptable e-mail usage. Achieve a culture of responsible e-mail usage at all levels of the organization.
Requirements:	
CF 5.4.1.	The site shall establish, implement and maintain an e-mail policy.
CF 5.4.2.	The policy shall include: • individual responsibilities and accountability, • what constitutes acceptable and unacceptable behavior, • formats approved for dissemination of information, • actions required should an inappropriate e-mail or suspected malicious code be received, • the consequences of unacceptable e-mail use, and • training and awareness requirements
CF 5.4.3.	The policy shall be communicated and a record maintained of the individual's understanding and acceptance of the content.

CF 5.5.	System Administrator and Elevated Privilege User Accounts
Objectives:	Define, control and securely manage persons with administrator/elevated privilege level access to network/systems and logical media assets
Requirements:	
CF 5.5.1.	The site shall establish, implement and maintain a policy to define, control and secure administrative and elevated privilege activities.
CF 5.5.2.	Default Admin accounts shall be renamed.
CF 5.5.3.	Administrators and privilege users shall use basic user accounts for normal day-to-day activities such as e-mail and authorized Internet access.
CF 5.5.4.	No email access is permitted for administrator accounts.
CF 5.5.5.	Administrator accounts are not permitted to visit external websites unless approved by management.
CF 5.5.6.	Administrative functions shall be approved by management and have individual account credentials to prevent compromise.
CF 5.5.7.	Administration account functions shall be monitored, logged and regularly audited. Records shall be retained for a minimum of three years.
CF 5.5.8.	The policy shall be communicated and a record maintained of the individual's understanding and acceptance of the content.

CF 5.6.	System Basic User Accounts
Objectives:	Define, control and securely manage persons with basic user level access to network/systems and logical media assets.
Requirements:	
CF 5.6.1.	The site shall establish, implement and maintain a policy to define, control and secure basic user activities.
CF 5.6.2.	Users shall have individual user accounts controlled by username and password credentials. See CF 5.7 Password Management.
CF 5.6.3.	Basic user accounts shall be configured to prohibit: • installing software, • uninstalling software, • modifying security software (e.g., anti-virus, firewall, IDS, etc.), • adding functioning hardware to the local system, • adding drivers to the system, • deleting accounts, • modifying network aspects of the system (e.g., IP address, etc.), • running any system/administrator/root type command, and • changing account permissions.
CF 5.6.4.	User accounts shall be disabled prior to notification of termination.
CF 5.6.5.	User accounts shall be reviewed on a regular basis to ensure that unauthorized accounts do not remain active.
CF 5.6.6.	Policy shall be communicated and a record maintained of the individual's understanding and acceptance of the content.

CF 5.7.	Password Management
Objectives:	Ensure the site has appropriate and consistent password controls to deter unauthorized access to IT systems.
Requirements:	
CF 5.7.1.	The site shall establish, implement and maintain a password policy.
CF 5.7.2.	Password format and complexity requirements must be established, set and monitored at administrator level.
CF 5.7.3.	Password expiry time shall be defined.
CF 5.7.4.	Criteria for re-use of passwords shall be defined.
CF 5.7.5.	Separate passwords shall be used for administrator, privileged and basic user accounts.
CF 5.7.6.	Education on password awareness shall be provided (also see CF 6 Training and Awareness).
CF 5.7.7.	Password selection and quality definition of the policy shall include individual responsibilities and accountability including the consequence of policy breach.
CF 5.7.8.	The policy shall be communicated and a record maintained of the individual's understanding and acceptance of the content.

CF 5.8.	Authorizing Third-party Access to IT Systems
Objectives:	To maintain integrity and security of IT systems/networks and logical media assets accessed by third-parties.
Requirements:	
CF 5.8.1.	The site shall establish, implement and maintain a policy and process for authorized third-party access.
CF 5.8.2.	Access shall be authorized, documented, monitored and reviewed.
CF 5.8.3.	Sites shall maintain third-party service legal agreements and review regularly for effectiveness.
CF 5.8.4.	Third-parties shall be required to adhere to the sites IT security policies and procedures.
CF 5.8.5.	The policy shall be communicated and a record retained of the companies' acceptance and individuals' acceptance and understanding of the content.
CF 5.8.6.	All parties shall sign non-disclosure and confidentiality agreements. Agreements shall be specific to the activity undertaken.

CF 5.9.	Removable Media
Objectives:	To ensure sites have controls on removable media to prevent unauthorized removal from the site or introduction of threats to IT systems.
Requirements:	
CF 5.9.1.	The site shall establish, implement and maintain a removable media policy.
CF 5.9.2.	The policy shall include individual responsibilities and accountability.
CF 5.9.3.	Unauthorized or non-essential devices shall be prevented from accessing the network.
CF 5.9.4.	Authorization criteria and a procedure shall be established.
CF 5.9.5.	A list of authorized devices shall be maintained.
CF 5.9.6.	Authorized devices shall be clearly identified and entered onto an asset register.
CF 5.9.7.	Policy shall be aligned to an ''end point'' security solution and network access controls.
CF 5.9.8.	Policy shall outline the consequences of any failure to comply.

CF 5.10.	Mobile Device Management
Objectives:	Set a formal requirement for mobile device acceptable use. Achieve a culture of responsible behavior when working with mobile devices.
Requirements:	
CF 5.10.1.	The site shall establish, implement and maintain a mobile device acceptable use policy.
CF 5.10.2.	The policy shall define rules pertaining to acceptable use and responsibilities of all users irrespective of association (i.e., employee, contractor or temporary staff).
CF 5.10.3.	The policy shall ensure that client assets are not stored on mobile devices.
CF 5.10.4.	Mobile devices shall be authorized for introduction to and removal from the site by a person responsible for system administration duties.
CF 5.10.5.	Where guards are used to prevent the introduction or removal of storage devices from the site, such devices shall be visibly marked and an inventory list held by the guards to verify the device is authorized.
CF 5.10.6.	All mobile devices shall be backed up on a regular basis to avoid loss of data.
CF 5.10.7.	All mobile devices shall be protected with malware and firewall software where appropriate.
CF 5.10.8.	Where technology exists, mobile devices shall be encrypted to prevent data migration if stolen or lost.
CF 5.10.9.	Mobile phones shall be PIN locked on timeout. Mobile devices shall be password protected on timeout.
CF 5.10.10.	Where an incorrect PIN is entered 5 times consecutively, this shall cause the device to lockout.
CF 5.10.11.	Where technology exists, the site shall have the ability to remotely lock, wipe or find devices when a device is reported stolen or lost.
CF 5.10.12.	Users shall sign adherence to policy.

CF 5.11.	Wireless Networks
Objectives:	Secure wireless networks to prevent unauthorized access or loss of sensitive data.
Requirements:	
CF 5.11.1.	The site shall establish, implement and maintain a wireless networks policy.
CF 5.11.2.	No wireless access shall be allowed into production or replication networks.
CF 5.11.3.	All wireless access shall be protected from unauthorized access.
CF 5.11.4.	All wireless signals shall be protected from information interception. As a minimum, WPA2 shall be implemented between infrastructure and client.

CF 5.12. Incident Management

Objectives: Ensure that sites can manage incidents effectively.

Requirements:

CF 5.12.1. The site shall establish and implement an incident management policy.

CF 5.12.2. Sites shall document plans for initial and extended triage as necessary to include methods for:

- monitoring,
- detection,
- root cause analysis,
- incident categorization, and
- incident prioritization.

CF 5.12.3. Roles and responsibilities shall be defined.

CF 5.12.4. The site shall manage and align the recovery from logical security incidents in line with CF 7 Business Continuity and Disaster Recovery Planning to include:

- containment,
- quarantine,
- evidence capture,
- removal,
- restoration, and
- corrective action.

CF 5.13.	Physical and Environmental Security Controls
Objectives:	Ensure data and logical media assets are physically controlled and secured. Ensure environmental conditions are managed.
Requirements:	
CF 5.13.1.	Sites shall establish adequate controls to physically protect and control access to servers and data stores.
CF 5.13.2.	Access shall only be given to authorized personnel based on a need to routinely access, visit, or work in the designated secure area.
CF 5.13.3.	Details of visitors to the secure locations shall be documented giving time date and purpose for the visit.
CF 5.13.4.	All visitors shall be escorted.
CF 5.13.5.	In the case of shared services the physical access to servers shall be secured using secured cabinets.
CF 5.13.6.	Keys and combinations shall be issued and retained by an appointed administrator.
CF 5.13.7.	Data stores (especially backup stores) shall be protected from poor environmental conditions, which include dust, dirt, smoke and strong electromagnetic fields. These may include fire and heat sensors, fire suppression, air conditioning, temperature controls, raised flooring, fire-rated wall and doors, etc.
CF 5.13.8.	Locations shall be inspected on a regular basis and subject to routine maintenance.
CF 5.13.9.	Uninterrupted power supply shall extend to all security and environmental controls protecting servers and data stores, and sized appropriately for local conditions and business activities.

CF 5.14.	IT Asset Management
Objectives:	Ensure the site has a register of all hardware, associated devices and software in use. Ensure that regular reviews of software use are undertaken. Ensure data from defective hardware is securely removed prior to any authorized repair. Ensure that redundant hardware and associated devices are disposed of properly in a secure manner that prevents data migration.
Requirements:	
CF 5.14.1.	There shall be a policy defined for the registration, management, use, repair and destruction of all hardware, associated devices and software.
CF 5.14.2.	Individual responsibilities and accountability shall be defined.
CF 5.14.3.	All assets and software shall be subject to an acceptance and 'authorization for use' process.
CF 5.14.4.	Authorized hardware and devices shall be clearly identified by visible marking through use of asset tags, bar codes or similar with the asset number entered onto the asset register.
CF 5.14.5.	All associated software authorized for use on each IT asset shall be documented within the asset register including details of license keys to prove authenticity.
CF 5.14.6.	The deployment of software on each workstation shall be reviewed on a regular basis by a person responsible for system administration to ensure that it has been authorized for use.
CF 5.14.7.	Policy shall be aligned to an ''end point'' security solution and network access controls.
CF 5.14.8.	There shall be an authorization for repair and disposal processes, controlled by a system administrator. Personnel shall not self-authorize removal from use, repair or destruction.
CF 5.14.9.	Hardware and associated devices identified as being redundant shall have all stored data wiped or destroyed prior to repair or disposal. Records shall be maintained for a period of three years.
CF 5.14.10.	Policy shall outline the consequence of a breach.

CF 5.15.	Network Monitoring
Objectives:	Ensure networks are monitored effectively.
Requirements:	
CF 5.15.1.	The site shall enable logging on all systems handling digital assets and develop a process to protect logs from change, review logs regularly and define a system to report findings and investigate anomalies. The logging shall include information relating to events and changes to security hardware and software and provide enough detail to allow effective investigation.
CF 5.15.2.	Controls shall be enabled to warn personnel responsible for system administration of any IDS/IPS suspicious activity.

CF 5.16.	Access Controls
Objectives:	Effectively manage access controls.
Requirements:	
CF 5.16.1.	The site shall establish a policy and system to ensure that only those persons authorized to access information systems and data are identified, authenticated and authorized before access to sensitive data is permitted.
CF 5.16.2.	The site shall establish and configure effective security technologies safeguarding sensitive data.
CF 5.16.3.	Sites shall establish mandatory access controls (MAC), discretionary access controls (DAC) and or role-based access controls (RBAC) to determine ownership and accountability for file and data.
CF 5.16.4.	Workstations shall be configured to lock out after a defined period of inactivity.
CF 5.16.5.	Controls shall be reviewed regularly.

CF 5.17.	Remote Access
Objectives:	Establish effective controls to secure remote access requirements.
Requirements:	
CF 5.17.1.	The site shall establish a policy and system to ensure that only those persons authorized to access information systems and data are identified, authenticated and authorized before access to sensitive data is permitted.
CF 5.17.2.	Sites shall establish mandatory access controls (MAC), discretionary access controls (DAC) and or role-based access controls (RBAC) to determine ownership and accountability for files and data.
CF 5.17.3.	Controls shall deny remote e-mail access through third-party web applications, e.g., Outlook Web Access.
CF 5.17.4.	Controls shall deny remote access through third- party applications, e.g.: • PCAnywhere, • Log-Me-In, • Windows Remote Assistance, and • non-encrypted remote desktop.
CF 5.17.5.	Where remote tele-working is approved, a minimum two-factor authorization VPN shall be established.
CF 5.17.6.	Controls must be reviewed regularly.

CF 5.18.	Change Management
Objectives:	Effectively manage change within the site's networks.
Requirements:	
CF 5.18.1.	The site shall establish and document a process to manage change to the information systems employed.
CF 5.18.2.	The site shall define with the documented process a method for recording significant changes, planning and testing of changes, assessment for potential impact, formal approval and communication of change to relevant persons.
CF 5.18.3.	Fallback procedures must be documented to mitigate the risk of unsuccessful changes.

CF 5.19.	System Documentation
Objectives:	Effectively document systems architecture of the site's networks.
Requirements:	
CF 5.19.1.	The site shall establish and implement or incorporate into existing policy a system architecture policy.
CF 5.19.2.	Policy shall define clear process for recording and presenting network landscapes.
CF 5.19.3.	Policy shall express security consideration and controls of such diagrammatical information.
CF 5.19.4.	A network landscape diagram shall be produced and held under secure conditions to prevent exposure of possible vulnerabilities.

CF 5.20.	External Networks
Objectives:	Maintain the security of external networks.
Requirements:	
CF 5.20.1.	All external content bearing network segments shall be monitored for anomalies.
CF 5.20.2.	All external connections shall be recorded and assessed based against business requirements and reviewed regularly.
CF 5.20.3.	Logs shall be retained for a minimum of 12 months.

CF 5.21.	Internal Networks
Objectives:	Maintain the security of internal networks. Ensure segregation of administrative functions
Requirements:	
CF 5.21.1.	All internal content bearing network segments shall be mapped and secured from unauthorized access.
CF 5.21.2.	All production, development and general network segments shall be segregated from each other.
CF 5.21.3.	Production segments shall have no direct connection to the Internet.
CF 5.21.4.	All network segments transporting content shall be monitored for anomalies.
CF 5.21.5.	Administration functions shall be adequately segregated to protect client assets.

CF 5.22.	File Transfer Management
Objectives:	Ensure effective file transfer methodologies and encryption.
Requirements:	
CF 5.22.1.	The site shall have a full understanding of each connection and documented process for recording access to or authorization for release of each employed technology.
CF 5.22.2.	Where key delivery messages (KDMs) are used, they shall be time specific and valid only for a specific destination device.
CF 5.22.3.	Where relevant, production and hosting environments shall provide verification of the file integrity using hash comparisons or equivalent.
CF 5.22.4.	Any encryption shall use/hold a valid certificate issued by a recognized authority.
CF 5.22.5.	Where portable drives are used to deliver client assets to a final destination, they shall be encrypted in line with industry best practice.
CF 5.22.6.	Such systems are to be recorded and any anomalies investigated and reported accordingly.
CF 5.22.7.	Sites shall establish internal audits for transfer of media.

CF 5.23.	Firewall Management
Objectives:	Ensure effective firewall management.
Requirements:	
CF 5.23.1.	All connections from outside the site (or larger corporate network) shall be controlled by a correctly configured firewall.
CF 5.23.2.	Application level firewalls must track both internal and external traffic.
CF 5.23.3.	Firewalls shall be configured to an agreed firewall policy as a minimum default setting to “Deny All.”
CF 5.23.4.	Establish an agreed state table for management of IP address ranges and port controls.
CF 5.23.5.	Firewalls must be capable of rejecting packets based on the state table.
CF 5.23.6.	Automatic alerts shall be enabled when a firewall configuration changes or re-boots. E-mail or SMS messages shall be sent to the person responsible for system administration and the cause of change or re-boot investigated.

CF 5.24. Vulnerability Management

Objectives: Ensure effective anti-virus is installed and maintained.
Ensure that vulnerabilities are reduced by regular security updating.
Ensure that server and system configuration back-ups are available in the event of an unplanned incident.
Ensure that data maintains integrity and confidentiality in the event of a loss of services.

Requirements:

CF 5.24.1.	An anti-virus policy shall be documented and implemented. All servers and workstations shall be protected or exceptions to deployment shall be justified.
CF 5.24.2.	Where exceptions to anti-virus deployment have been made, alternative methods for protection must be defined.
CF 5.24.3.	Anti-virus software shall be updated at least weekly on workstations and daily on servers.
CF 5.24.4.	Anti-virus shall not be capable of being disabled by basic users.
CF 5.24.5.	Anti-virus shall perform on access scanning and scheduled background scanning at least monthly on workstations and weekly on servers.
CF 5.24.6.	Anti-virus shall, as minimum, quarantine suspicious files.
CF 5.24.7.	There shall be a documented patching regime for servers, workstations and security barriers.
CF 5.24.8.	All servers and workstations shall be patched at least quarterly; security barriers shall be patched at least monthly.
CF 5.24.9.	All justifications for non-patching must be documented and justified.
CF 5.24.10.	All public facing and internal servers shall be base-lined, their configuration defined, recorded and backed-up to external storage media, stored under secure conditions.
CF 5.24.11.	All unnecessary services shall be removed or disabled from all servers.
CF 5.24.12.	Public facing servers shall not have any internal facing credentials stored. Internal facing servers shall not have access to the internet.
CF 5.24.13.	Client data and sensitive/valuable company data shall be backed up off site on a regular basis to ensure availability of data in the event of an unplanned incident.
CF 5.24.14.	The site shall provide evidence of vulnerability assessment and shall consider an appropriate level of testing to be applied according to documented risk assessment.

CF 6. TRAINING AND AWARENESS

CF 6.1. Training and Awareness Needs

Objectives: Ensure all personnel are trained and made aware of security requirements.

Requirements:

CF 6.1.1.	The site shall establish a policy to ensure that security training is effectively delivered.
CF 6.1.2.	Awareness of site security measures and requirements shall be provided.
CF 6.1.3.	Security training and awareness shall be made available to all and shall be provided as required according to role and responsibility.
CF 6.1.4.	As a minimum, security awareness shall be delivered to all new starters, contractors and temporary staff, and thereafter delivered annually to maintain such awareness.
CF 6.1.5.	Specific security requirements of the CPS Standard, legal, regulatory and contractual obligations shall be identified, reviewed and incorporated into a structured training program.
CF 6.1.6.	The site shall ensure that records of attendance are maintained.

CF 6.2.	Basic Users and Elevated Privilege Users
Objectives:	Ensure all personnel are trained and made aware of IT security requirements and current risks operating in a media IT environment.
Requirements:	
CF 6.2.1.	All users with access to physical or digital assets shall undergo initial education and annual IT and digital security refresher training of minimum 30 minutes duration. User training shall cover: • current internet security threats, • good password selection, use and storage, • identifying and responding to social engineering and phishing attacks, • acceptable use of email, • use and benefits of encryption, • safe and responsible web browsing and social networking, • use and benefits of anti-virus, • protecting, sharing, storing and destroying data, • securing the desktop, • securing the laptop, • mobile device security, • Wi-Fi security and encryption, • working remotely, and • home networking and personal computer use.
CF 6.2.2.	Users must be aware of site policies and procedures for IT security relevant to their role.
CF 6.2.3.	Users must also be aware of the current risks when operating in a media IT environment.
CF 6.2.4.	Elevated privilege users/administrators must receive both basic and specialist training specific to the added responsibilities they hold. This may include the attendance of external training programs. Administration training shall consider the following: Physical Security: • basic principles of physical security, • use and management of authorized access controls, • use and management of CCTV,

CF 6.2. Basic Users and Elevated Privilege Users

- management of intrusion detection,
- use and management of environmental controls, and
- log capture and retention.

Operating Systems and Device Management:

- installing devices on the LAN,
- optimizing devices,
- controlling access across the LAN to the device,
- backup and storing configuration files,
- auditing device configuration
- secure remote management of a device,
- patching and device update,
- installing the operating system from a reliable source,
- optimizing operating system performance,
- controlling access across the LAN to the platform,
- adding users,
- controlling user access (e.g., temporary, power or root level),
- limiting user access (permissions and profiles),
- restricting times of access,
- controlling account expiry, and
- patching the operating system.

Network Security:

- protocol stack and IPv4 limitations,
- confidentiality, integrity and availability (CIA) security concepts,
- defining vulnerability,
- defining an exploit and how they can affect the organization's network,
- understanding the importance of patching,
- controlling access across the LAN to assets/data/information,
- backup and storing data securely,

CF 6.2. Basic Users and Elevated Privilege Users

- basic auditing of network security,
- use of applications (e.g., nMap and Nessus) to assist identification of common configuration and security issues,
- reporting, recording and correcting security issues,
- network scanning and legal implications, and
- achieving network defense in depth, providing the understanding of how to control access to public services, harden servers and secure the internal network.

Use and application of complementary technologies to increase security, such as:

- intrusion detection systems (IDS),
- intrusion prevention systems (IPS),
- firewalls,
- threat management tools,
- wireless attack detection systems,
- network access control,
- anti-virus management,
- secure web proxy devices,
- secure mail proxy devices,
- multi-factor identification,
- multi-factor authentication, and
- encryption.

Firewall Configuration:

- selecting and installing a firewall,
- identifying and adding rules necessary for secure configuration,
- controlled access across the LAN to the device,
- backup and storing configuration files,
- auditing the configuration of the device, and
- managing secure remote access.

Wireless Configuration:

- installing the device,
- optimizing and controlling the power of the device for the environment,

CF 6.2.	Basic Users and Elevated Privilege Users

- controlling access across the LAN to the device,
- backup and storing configuration files,
- implementing security on the device WPA –WPA2,
- implementing structure or enterprise (RADIUS),
- auditing wireless configuration, and
- managing secure remote access

Secure Asset Disposal Policy:

- tracking items sent for disposal,
- log retention
- hard disk drive destruction.

CF 6.3.	Dedicated and Skilled IT Security Staff
Objectives:	Ensure sites consider the training requirements for skilled security staff and where feasible appoint a dedicated IT security role.
Requirements:	
CF 6.3.1.	The site shall provide specific IT security training to support administrative functions.
CF 6.3.2.	The site must consider the feasibility of a dedicated IT security role independent of the network support team.
CF 6.3.3.	The decision not to appoint a dedicated IT security role must be evidenced by management.

CF 6.4.	Training Records
Objectives:	Design and produce a security policy manual and associated documentation. Communicate all security policies, procedures and work instructions to staff. Ensure documents remain current and fit for purpose through a process of review.
Requirements:	
CF 6.4.1.	Records of security training shall be maintained and retained for a minimum of three years.
CF 6.4.2.	Records shall include details of training package content, name of the instructor, and dates of training and results of any examinations or assessments.

CF 6.5.	Personnel Participation
Objectives:	Develop a responsible and secure culture and provide opportunity to participate in improving site security.
Requirements:	
CF 6.5.1.	Management shall encourage employee participation in the content security management system, including security process planning and implementation, the detection of security breaches and the identification of improvement opportunities where appropriate.
CF 6.5.2.	Management shall provide methods for employees to report security issues without fear of retribution.

CF 7. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

CF 7.1. Business Continuity Plan (BCP) and Disaster Recovery Planning (DRP)

Objectives: To ensure the confidentiality, integrity and availability of client assets are maintained in the event of an unexpected or significant disaster, event or emergency.
To minimize the impact on clients in the event of an unexpected or significant disaster, event or emergency.

Requirements:

CF 7.1.1. A BCP and DRP shall be established and published.

CF 7.1.2. Sites shall identify a role to manage BCP and DRP activities.

CF 7.1.3. Policy and plans shall be communicated to all employees.

CF 7.1.4. The BCP and DRP shall include:

- likely physical, technical and human scenarios,
- critical systems and processes,
- key individuals and critical assets,
- high level stages and outlined plans to secure assets, stabilize and recover operations,
- links to CF 1.2 Risk Management.

CF 7.1.5. The site shall establish regular reviews of BCP and DRP plans and processes.

CF 7.1.6. The site shall establish effective methods for testing these plans.

CF 7.1.7. Sites shall document findings of reviews and tests, and update the plan accordingly.