Content Delivery & Security Association

Content Protection & Security Standard

Governance and Security Culture

Personnel and Resources

Asset Management

Physical Security

IT Security

Training and Awareness

Business Resilience

Content Protection & Security Program

Revised: February 2016

ABOUT THIS STANDARD

The CPS Standard has been established to secure media assets at all stages of the supply chain. This objective-based approach examines seven frameworks of capability.

CONTENT PROTECTION AND SECURITY STANDARD

- **CF 1: GOVERNANCE AND SECURITY CULTURE**
- **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 RESILIENCE**

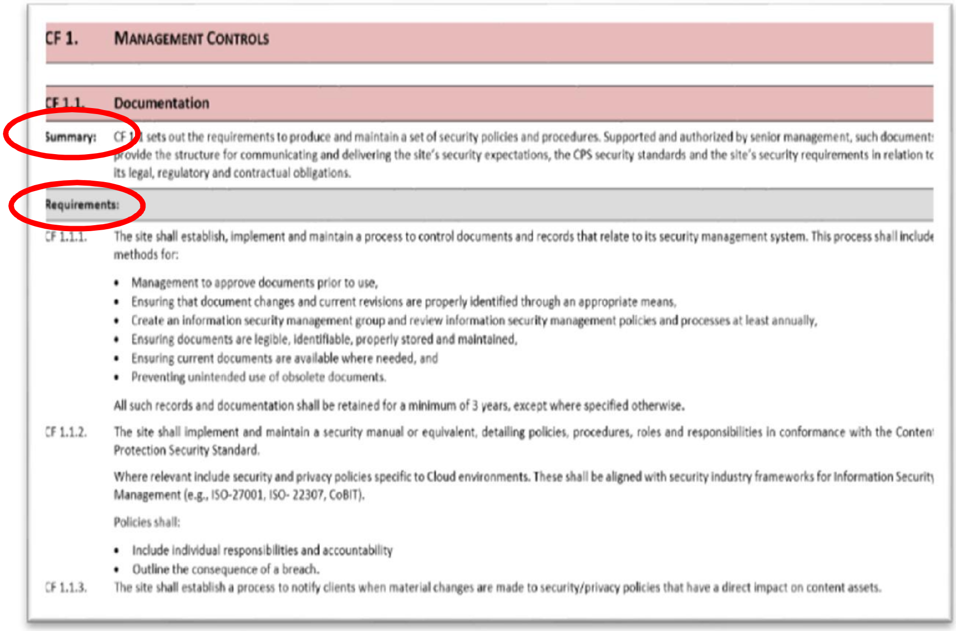
The requirements defined within the Standard and its accompanying guidance form the basis of a Content Security Management System (CSMS). This consists of a series of controls designed to assess, manage and minimize risk to an acceptable level, thereby ensuring the continued confidentiality, integrity and availability of intellectual property and media assets.

CDSA have considered industry specific risk, identified current threats and vulnerabilities that are encountered within the industry. This process has facilitated the formulation of a suite of security objectives to control and/or mitigate those risks, threats and vulnerabilities.

These objectives define the auditable requirements for CDSA Content Protection and Security (CPS) program certification.

CDSA recognize and acknowledge the relevance and importance of other security standards and industry best practice. Where relevant, specific reference and acknowledgement has been made within the content of this Standard and Guidance documentation.

Within each section, a summary is provided to assist you with your preparation. Guidance and support is available from your appointed CDSA auditor or Territory Director throughout. The example below illustrates the layout of each section of the Standard.



CF 1. MANAGEMENT CONTROLS

CF 1.1. Documentation

Summary: CF 1.1 sets out the requirements to produce and maintain a set of security policies and procedures. Supported and authorized by senior management, such document provide the structure for communicating and delivering the site's security expectations, the CPS security standards and the site's security requirements in relation t its legal, regulatory and contractual obligations.

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:

- Management to approve documents prior to use,
- Ensuring that document changes and current revisions are properly identified through an appropriate means,
- Create an information security management group and review information security management policies and processes at least annually,
- 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 implement and maintain a security manual or equivalent, detailing policies, procedures, roles and responsibilities in conformance with the Conten Protection Security Standard.

Where relevant include security and privacy policies specific to Cloud environments. These shall be aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO- 22307, CoBIT).

Policies shall:

- Include individual responsibilities and accountability
- Outline the consequence of a breach.

CF 1.1.3. The site shall establish a process to notify clients when material changes are made to security/privacy policies that have a direct impact on content assets.

Declination of Liability

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

CF 1. GOVERNANCE AND SECURITY CULTURE

CF 1.1. Security Management

Summary: CF 1.1 sets out the requirements for introducing effective Governance and Security Culture. Participants should apply a pyramid of security controls, supported and authorized by senior management, providing the structure for communicating and delivering the participant's security expectations, the CPS security standards and the participant's security requirements in relation to its legal, regulatory and contractual obligations.

Requirements:

CF 1.1.1. The Participant shall ensure that Board of Directors and Senior Executives understand their responsibility for Security Governance. The Participant shall demonstrate that the following essential practices are applied:

- Security in on the Boards Agenda.
- Security Leaders have been identified, are held accountable for compliance and are supported by the Board in their role.
- Security performance is subject to review and approval to ensure continued effectiveness.
- An information security management group has been established to review information security management policies and processes at least annually.

CF 1.1.2. The Participant shall implement and maintain a security manual or equivalent, detailing policies, procedures, roles and responsibilities in conformance with the Content Protection Security Standard.

Where relevant include security and privacy policies specific to Cloud environments. These shall be aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO- 22307, CoBIT).

Policies shall:

- Include individual responsibilities and accountability
- Outline the consequence of a breach.

CF 1.1.3. The participant shall establish, implement and maintain a process to control documents and records that relate to its security management system. All such records and documentation shall be retained for a minimum of 3 years, except where specified otherwise.

CF 1.1.4. The participant shall establish a process to notify clients when material changes are made to security/privacy policies that have a direct impact on content assets.

CF 1.2. Risk Management

Summary: CF 1.2 sets out the requirements for Risk Assessment and Management Controls. Participants are required to undertake and document risk assessments for each activity that relates directly or indirectly to the security of media assets. Consideration is to be given to the use of third party vendors, relevant legal, regulatory and contractual obligations. Risks must be identified, classified according to the level of threat and mitigated to an acceptable level. The risk assessment is used to map the applicability of the CPS Standard according to the services and activities performed.

Requirements:

CF 1.2.1. Management shall define roles and responsibilities for risk assessment.

CF 1.2.2. Risk assessments shall be documented, describing each risk, analyzing its level of impact and assessing the likelihood of a security incident occurring.

CF 1.2.3. A methodology for risk assessment shall be provided.

CF 1.2.4. A risk register that identifies all security risks to content shall be created and maintained.

CF 1.2.5. Risk assessments shall be reviewed by senior management annually, following a security incident or before significant changes in business activity.

CF 1.3. Compliance

Summary: CF 1.3 sets the requirements for Compliance, Incident Management. Participants are required to provide assurance of capability to detect and respond to security incidents and recover from them in timely manner. CF 1.3 also sets requirements for Internal Auditing..

Requirements:

CF 1.3.1. The participant shall create a security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.

CF 1.3.2. The participant shall establish, implement and maintain a procedure and workflow for security incident monitoring and response.

CF 1.3.3. The participant shall establish, implement and maintain corrective and preventive action processes.

CF 1.3.4. Internal audit procedures shall be established, implemented and maintained to ensure:

- The participant complies with the CPS Standard and any legal, regulatory or contractual obligations,
- Internal audits are scheduled and performed at least once per year, no later than six months following the CDSA external audit,
- Where practicable, persons carrying out the audit are independent of those responsible for the activity,

CF 1.3.	Compliance
	• Results of the audits are recorded and published to allow those responsible to make corrective or preventive actions.

CF 2. PERSONNEL AND RESOURCES

CF 2.1. Personnel and Resources

Summary: CF 2.1 sets out the requirements for personnel and resource security management. A dedicated program manager shall be appointed. Allocated and segregated security functions must be in place to achieve security objectives. Management shall apply appropriate and proportionate levels of background screening to be carried out on all personnel and resources, including contractors, consultants and third-party vendors. The participant must be capable of providing personnel and resources to meet the requirements of the CPS Standard, legal, regulatory and contractual obligations.

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.

The responsibilities and authorities of all management involved in the security management system shall be defined and documented.

CF 2.1.2. The participant shall document and implement personnel security processes that align with the organization’s current information security procedures.

CF 2.1.3. Contracts of employment should include a requirement to comply with security policy, procedures and processes.

CF 2.1.4. Management shall ensure that areas of responsibility are separated where necessary to reduce opportunities for unauthorized modification and misuse of information or services.

CF 2.1.5. Management shall identify and ensure the availability of adequate budget for mandated security requirements.

CF 2.2. Third-party Resources

Summary: CF 2.2 sets out the requirements for dealing with third-party resources, contractors and companies such as agents, offload partners and support services. Management is required to consider, as a minimum, the implementation of policy, procedures, Service Level Agreements, non-disclosure agreements and confidentiality clauses within contracts. The participant must be capable of providing documented policies and procedures to meet the requirements of the CPS Standard, legal, regulatory and contractual obligations.

Requirements:

CF 2.2.1. The participant shall have secure processes for the contracting and engagement of any third-party resources conforming to relevant CDSA requirements. Management shall ensure that appropriate Service Level Agreements (SLAs) and contractual obligations are agreed, implemented and reviewed regularly.

CF 2.2.2. Participants are required to notify clients if subcontractor companies are used to handle content assets and should require subcontractors to go through standard due diligence activities

CF 2.2.3. Participants are to ensure that subcontractors comply with security contractual obligations as stipulated by the content asset owner.

CF 2.2.4. For Cloud environments participants shall establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/data once the client contract has terminated.

CF 3. ASSET MANAGEMENT

CF 3.1. Administrative Controls

Summary: CF 3.1 sets out what is required to establish and communicate the roles and responsibilities for asset management. Specific consideration is to be given to the types of asset being handled.

An asset may be defined as:

- intellectual property, content including edits, rough cuts, un-mastered and mastered content, proprietary or sensitive information, work in process or finished product,
- including the media or device (e.g., flash drives, Pro-tools/portable drives, USB, CD, DVD, AIT, DAT, DLT, etc.) on which it is received, handled or stored when under the control of the organization, and
- may take a physical, digital or electronic form and may exist at any point in the supply chain, such as, but not exclusively: content creation, work in process, editing, digital compression, encoding and authoring, manufacturing, distribution, destruction and deletion.

Clear, concise, documented policies and procedures must be communicated to staff, defining how assets are to be handled at each stage. Each activity must be documented, outlining any special requirements necessary for ensuring the security of an asset. Each project is to be considered on the basis of risk and value, outlining any special requirements for ensuring that integrity is maintained and legal, regulatory and contractual requirements are met.

Administrative control of computer systems and storage locations containing digital IP or other commercial assets must be considered.

These controls provide the basis for a Chain of Custody (CoC) of all assets while in the participant’s custody.

Requirements:

CF 3.1.1. The participant shall introduce an asset management system which may be either electronic or paper-based capable of providing an auditable chain of custody, identifying the location and time/date of creation, movement or destruction.

CF 3.1.2. Management shall define secure processes, in accordance with risk assessment and client requirements for each stage of asset handling. Such processes shall ensure the security of content stored on both physical and digital media, including reference copies, temporary storage and backups of content.

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. Each risk category shall have assigned specific security handling, storage and transportation.

CF 3.1.4. Storage media and digital file names should be anonymized and contain no reference to the file content.

CF 3.1.5. For cloud environments establish procedures for labeling, handling, and securing containers that contain data and other containers.

CF 3.2. Asset Handling and Transfer

Summary: CF 3.2 sets out the requirements for procedures and workflows to ensure that all assets are handled and transferred in a secure, consistent and auditable manner.

Requirements:

CF 3.2.1. Ensure all asset movement, both physical and digital is recorded, auditable and reviewed throughout the assets' chain of custody.

CF 3.2.2. Ensure that security techniques are available for use and are applied when instructed. e.g., spoiling, invisible/visible watermarking

CF 3.2.3. Participants shall:

- Control and restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.
- Assign unique username and passwords to portal users and distribute these credentials securely.
- Ensure users only have access to their own digital assets.

CF 3.2.4. For cloud environments, establish, document and implement scenarios to clients in which client content/data may be moved from one physical location to another.

CF 3.2.5. For cloud environments participants shall provide:

- Clients with information regarding locations for their content assets and data.
- The capability to control the physical location/geography of storage of a client's content assets and data if requested.

CF 3.3. Secure Asset Storage and Reconciliation Controls

Summary: CF 3.3 The participant must ensure that assets are retained securely within designated and segregated areas with regular supervisory checks conducted to ensure accuracy, integrity and security are maintained. The use of cyclic counting provides an auditable mechanism for compliance.

Requirements:

CF 3.3.1. The participant shall:

- Perform quarterly cyclic counts for stored client physical assets, where possible using employees independent of the asset management process
- Ensure that management review cyclic count procedures and results
- Ensure that discrepancies are investigated in line with CF 1.3 and reviewed by management
- The site shall allocate assets to secure physical or digital storage locations

CF 3.3. Secure Asset Storage and Reconciliation Controls

CF 3.3.2. Notify clients of discrepancies and the results of investigations.

CF 3.4. Asset Re-call Procedures

Summary: CF 3.4 sets out requirements for monitoring assets once allocated to an individual. Dependent on the activity and type of asset, different procedures may exist. However, the participant must take into consideration the risk to high security items. Procedures must address time lines prior to further investigation. Where discrepancies, inconsistencies or criminality are identified, the result of any investigation must be reviewed and consideration given to notifying the asset owner. Any process must comply with any legal, regulatory or contractual obligations.

Requirements:

CF 3.4.1. The participant shall adopt a procedure for asset recall, identifying criteria for items according to risk assessment. Where an asset cannot be accounted for, a person responsible for the activity shall conduct an initial investigation to recover the item.

CF 3.4.2. 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 3.4.3. Should an asset remain missing beyond an initial investigation, further inquiry shall be commenced using a person independent of the activity.

CF 3.4.4. A procedure for escalation and client notification shall be in place, compliant with any service level agreements or contractual requirements

CF 3.5. Control of Blank Media Materials

Summary: CF 3.5 sets out the requirements for controlling stocks of blank media material. Unless properly controlled access to blank media materials provides an opportunity to transfer, copy or transmit media files without detection. Blank media materials must be uniquely identified and stored in a secure location with restricted access.

Requirements:

CF 3.5.1. The participant shall ensure all blank media is:

- Tagged and logged upon arrival. Whenever possible, it shall be uniquely identified.

CF 3.5. Control of Blank Media Materials

- Stored in a secure location and access restricted to authorized personnel.

CF 3.5.2. The participant shall document an:

- Asset identification process for all blank media arriving on site.
- Authorization and tracking process for signing out all blank media for use.

CF 3.6. Record Retention

Summary: CF 3.6 The use of records provides management with an opportunity to ensure processes are being undertaken according to requirements. They may also provide evidence at audit that activities have been undertaken satisfactorily or provide information to investigate an incident in the event of an unplanned release, loss or theft of an asset. The meticulous retention of asset receipt records, asset handling documentation and asset tracking records forms part of the layered approach to security. Records are to be stored securely in line with the requirements.

Requirements:

CF 3.6.1. The participant shall establish a procedure for record retention. As a minimum, this shall include all asset receipt/dispatch records, manufacturing process documentation and asset tracking records.

CF 3.7. Transportation of Assets

Summary: CF 3.7 The secure transportation of assets off-site will vary according to the type of activity, asset, technology, destination and contractual obligation. However, the participant must possess a policy, procedure and work flow that mitigate risk and takes into account the vendor’s responsibility. As packaged goods represent a ‘finished article,’ the risk of financial loss is always considered high. Unfinished products may in some cases carry a lower financial risk, but all circumstances carry a reputational risk. Whatever the circumstance or method of carriage, whether it be the participants own transportation or a contracted third-party, a secure process must be evidenced to ensure compliance with the program.

Requirements:

CF 3.7.1. The participant shall establish procedures for the secure transportation of assets.

CF 3.7.2. Assets must be prevented from leaving a site until all checks and authorities for shipment have been met.

CF 3.7. Transportation of Assets

CF 3.7.3. Participants shall determine when and how vehicles shall be secured for shipping, according to documented risk assessment and client contractual obligations.

CF 3.7.4. Management shall ensure:

- Visiting drivers do not enter the premises, or, where necessary, are escorted at all times.
- Drivers do not park unsecure and unattended during delivery journeys.

CF 3.7.5. Participants shall apply appropriate security to shipped client assets.

CF 3.7.6. 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 3.8. Destruction and Recycling

Summary: CF 3.8 set out requirements for the destruction and recycling of assets. During the production or manufacturing process, physical assets are often created that require secure and responsible destruction. In certain cases, rejected assets are re-used to reduce costs and improve efficiency. For example, optical discs are often re-used and over-printed in the manufacturing process. Unless strictly controlled, this presents opportunities for compromise or loss of the asset.

Management must ensure that the retention and re-use of unwanted or redundant assets are reduced to a minimum and that assets are properly accounted for and secured prior to destruction or recycling. Management controls, enhanced security measures and meticulous record keeping are required to achieve security objectives. Where assets are re-used at a later stage to reduce set-up costs, efforts need to be taken to ensure that the content cannot be accessed or used afterwards.

Requirements:

CF 3.8.1. The participant shall implement and maintain secure processes for destruction and recycling of physical assets. Processes shall ensure that assets are rendered unusable and/or securely stored within suitable locked and marked containers while in production and manufacturing environments and while awaiting secure destruction.

CF 3.8.2. 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. While awaiting secure destruction, assets must be securely stored and monitored.

CF 3.8.3. Detailed records shall be maintained for all assets destroyed. A certificate of destruction must be made available for clients wishing formal conformation.

CF 3.8.4. Where on-site grinders and/or technology are used, they shall be monitored by CCTV.

CF 4. PHYSICAL SECURITY

CF 4.1. Physical Security Management

Summary: CF 4.1 sets out the requirements for physical security management. A documented plan must define the levels and types of physical security controls Implemented. Policy and procedures demonstrate how the participant detects, mitigates and responds to any given security risk, threat or incident. The type of controls used at each location must be reflected in a risk assessment process as defined in section CF 1.2 of this guide. Correct application of risk assessment is crucial to ensuring proportionate and effective controls are maintained.

Requirements:

CF 4.1.1. The participant shall establish and communicate a physical security plan which demonstrates that risk to personnel, media assets and the physical environment have been properly assessed and that controls are in place to reduce risks to an acceptable level. As a minimum, the plan shall include:

- site and internal 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 procedures, incident prevention, detection and response.

CF 4.2. Perimeter Security

Summary: CF 4.2 sets out the requirements for perimeter security measures. A perimeter may be defined by a combination of physical or natural boundaries, and may include features such as fences, walls, the outer walls of a building or by divisions inside it such as walls, gates and doors. The function of a perimeter boundary is to provide physical delineation where authorized access is required and presents a strong deterrent to intrusion or unauthorized access. Perimeter security is the first line of physical defense when safeguarding media assets. Irrespective of size and location, the participant must ensure that a physical boundary exists, that it is monitored and incidents can be responded to when a suspected or actual breach occurs. Its effectiveness must be reviewed regularly.

Requirements:

CF 4.2.1. The participant shall demonstrate its capability to secure the physical perimeter. The site shall be protected by a continuous physical barrier that is monitored and inspected regularly.

CF 4.2.2. All entry and exit points shall be secured and monitored using appropriate means to ensure only authorized access is permitted.

CF 4.2. Perimeter Security

CF 4.2.3. Where participant share building facilities, controls shall ensure that physical segregation is applied to maintain the integrity of secure areas.

CF 4.3. Securing Internal Areas

Summary: CF 4.3 sets out the requirements for defining, segregating and securing internal areas, in line with CF 4.1. Several layers of security must be demonstrated.

Secure locations may include:

- replication, mastering, manufacturing, printing, packing and distribution,
- stores, vaults, safes and libraries,
- recording, mastering and mixing studios,
- post production digital and testing facilities, and
- data centers and server locations.

A controlled area is considered to be a location where monitoring is required but no access to physical or logical assets is possible. A secure area is considered to be a location where monitoring, supervision and controlled access are required to protect physical or logical media assets. Media assets stored, handled, processed, manufactured, received or dispatched within a designated secure area have additional physical security requirements. Where practicable, assets are to be located in the less accessible parts of a floor or building.

Requirements:

CF 4.3.1. The participant shall demonstrate its capability for secure access, the monitoring and controlling of internal locations and secure areas.

CF 4.3.2. Authorized access to secure internal areas for personnel shall be established according to their roles and responsibilities, business need and a principle of least privilege.

CF 4.3.3. The possession and use of personal photographic, recording, storage and audio devices (including smart phones) shall be controlled when operating or visiting secure internal areas, subject to risk assessment. Where there is a significant risk to content they shall be prohibited.

CF 4.4. Use of Guards

Summary: CF 4.4 sets out the requirements for the use of guards. The use of guards is dependent on risk assessment. A decision to instruct guards is decided by level of risk, access to media assets and the availability of alternative controls, security systems or technology.

Where deployed, guards duties may include the following:

- To deter unauthorized intrusion to the site being protected, or if deterrence fails, to detect intrusion as early as possible and to report the incident to the relevant authorities.
- supervise the arrival and departure of vehicles,
- control and issue keys,
- inspect and check perimeter security by means of randomized patrol,
- inspect and check internal security by means of randomized patrol,
- manage and monitor CCTV,
- manage and monitor physical intruder detection systems (IDS) and perimeter lighting,
- manage and monitor visitors, employees, contractors and consultants,
- manage and monitor access control, and
- control entry/exit in/out of controlled and secure areas including checking ID and searching personnel, vehicles and bags.

Requirements:

CF 4.4.1. The participant shall implement and maintain an agreed set of assignment instructions for guards employed by the participant, subject to SLA and periodic management review. This should include effective processes to deal with perceived threats, including response and reporting plans. Where third-parties are used, requirements set out in CF 2 shall be followed.

CF 4.5. Searches

Summary: CF 4.5 sets out requirements for conducting searches of employees, visitors, and contractors exiting secure areas. A requirement to carry out searches is mandatory unless following a risk assessment, a decision not to search has been justified and documented within the statement of applicability. Companies working with physical media assets such as replication, warehousing and distribution facilities, must maintain a random search program that is proportionate to the risk. The geographic location, type of service, type of asset, legal, regulatory and contractual requirements will dictate the frequency of searches and whether or not to decline the implementation of search procedures.

Requirements:

CF 4.5.1. Searching of all persons and vehicles entering or exiting a designated secure area should be conducted unless the risk to content has been assessed and mitigated.

CF 4.5.2. A process for escalating a positive search and recording search details shall be adopted.

CF 4.5.3. A record of searches shall be made and retained for a minimum period of 90 days.

CF 4.6. CCTV

Summary: CF 4.6 sets out the security requirements for the use of closed circuit television (CCTV). Industry standards for acceptable use and retention of images are to be used to assist immediate response and post-incident reporting.

CCTV assists to protect:
- the perimeter boundary,
- internally controlled and/or designated secure areas, and
- physical and logical media assets.

Correct use captures:
- acts of criminality, and
- breaches of health and safety.

CCTV locations extend, improve and corroborate other security systems such as:
- patrolling guards,
- intruder detection, and
- automated access control.

As a guide images should be:

- reviewed annually to ensure continued quality for evidential purposes,
- fairly and lawfully processed,
- used for specific limited purposes such as the prevention and detection of crime,
- assessed as accurate, adequate, relevant but not excessive,
- retained only for as long as necessary and where law allows for 90 days minimum,
- processed in accordance with an individual’s human rights, and
- kept secure and only accessible by those who have a business need

CF 4.6. CCTV

Requirements:

CF 4.6.1. CCTV shall be used, subject to local laws and regulations, to aid the protection of content and placed to support access control, guard activities and searches.

CF 4.6.2. CCTV Images are to be:

- Time and date stamped
- Retained for a minimum of 90 days
- Only accessed by persons with legitimate business need.
- Monitored using suitably qualified staff Images shall be accurately time and date stamped.

CF 4.7. Lighting

Summary: CF 4.7 sets out the security requirements for the use of lighting to deter intrusion and reduce an intruders freedom of movement, to provide light to assist the detection of intruders and support other detection methods.

Requirements:

CF 4.7.1. Lighting should not be used to illuminate guards or patrols.

CF 4.7.2. Lighting should be used to aid CCTV imagery.

CF 4.7.3. Light schemes to be considered are:

- Perimeter Lighting
- Glare Lighting
- Area Lighting
- Asset Lighting
- Event Activated Lighting
- Entrance/Check Point Lighting
- Displacement Lighting
- Non-Visible Lighting
- Guardhouse Lighting

CF 4.7. Lighting

CF 4.7.4. Lighting should be subject to both preventative and corrective maintenance to ensure continued effectiveness

CF 4.8. Access Control Systems, Automated Technologies (AACS) and Key Management

Summary: CF 4.8 sets out the security requirements for the use access control systems, automated technologies (AACS) and key management. In some cases the implementation of proper key control continues to provide adequate control and mitigation of risks. Risk assessment drives the decision on the correct type of control to apply. Where possible the use of technologies allows organizations to affect entry and exit without physical intervention or supervision being used. Types of AACS may include physical token, keypad entry, proximity card reader and biometric readers. Such systems can be operated in isolation or in conjunction with each other and combined with other technology such as CCTV and alarm systems.

Requirements:

CF 4.8.1. The participant shall implement and maintain secure access control systems including managing system failure, tampering or avoidance.

CF 4.8.2. Events and movements to secure (restricted) areas shall be capable of being monitored, logged and available for immediate review.

CF 4.8.3. The participant shall implement a physical key management system to maintain security of keys, locks, security combinations and cabinets.

CF 4.9. Intruder Detection Systems (IDS)

Summary: CF 4.9 sets out the requirements for the use of Intruder Detection Systems (IDS). Use of IDS must be considered in areas that are left vulnerable when unattended, or when it is necessary to augment additional physical security barriers. Properly managed installation, maintenance, monitoring and response are essential requirements to success. When correctly installed, performance tested and employed, IDS can result in savings in human security resources.

Requirements:

CF 4.9.1. The participant shall implement, monitor and control a secure intruder alarm system subject to risk assessment. Event logs shall be retained for a minimum of 90 day and be available for review.

CF 5. IT SECURITY

CF 5.1. Information Security Management

Summary: CF 5.1 sets out the requirements for inclusion of IT security policy and procedures within an Information Security Management System (ISMS). Effective implementation of ISMS enables the participant to define the direction and commitment to managing and reducing IT security risks. The overarching ISMS forms the framework for IT security policy. The specific policy sections contain relevant controls and express senior management's commitment to safeguarding IT systems and logical media assets using skilled and properly trained resources. It also explains how security requirements are met relevant through applicable legal, regulatory and contractual obligations.

The ISMS refers to the technical security controls and practices employed to secure enterprise information systems. IT infrastructure consists of the equipment, systems, software, and services used in common across an organization including all hardware, networks and facilities required to develop, test, deliver, monitor, control and support IT services. IT Infrastructure also serves as the foundation upon which program or project-specific systems and capabilities are built.

Requirements:

CF 5.1.1. IT Security Policy (including cloud environments where applicable) shall be defined and communicated, covering the scope of CF5 IT Security

CF 5.1.2. A record shall be maintained of the individual IT users understanding and acceptance of their responsibilities under the IT Security Policy.

CF 5.1.3. IT security policy shall comply with the requirements of CF1.1 Documentation.

CF 5.2. Acceptable Use

Summary: CF 5.2 sets out the requirements for acceptable use of IT systems and logical media assets. Acceptable use is a rule set defined by the participant that restricts the way in which IT systems, networks and assets may be used. Acceptable use requirements assist to control everyday system and network activity. Such requirements must be defined and communicated to all persons who have access to the participant's information systems and include the purpose, authorization, privacy, behaviors and definition of what is and is not acceptable usage within any legal constraints. (already covered in CF1/2)

Requirements:

CF 5.2.1. Appropriate technical controls shall be implemented to support the requirements of the IT Security Policy in relation to the acceptable use of IT assets, email system and internet access.

CF 5.2. Acceptable Use

CF 5.2.2. The technical controls should be such that unauthorized transmission of client media assets is restricted as far as practicable, and attempts to do so are alerted to management

CF 5.3. System Administrator and Elevated Privilege User Accounts

Summary: CF 5.3 set out the requirements for administrator and elevated privilege IT system users with a level of access higher than those of a normal user. These would include power users, local administrators, domain administrators and enterprise administrators. In a traditional Unix or Linux environment persons with root level access are considered administrators.

See CF 6 for training and awareness requirements.

Requirements:

CF 5.3.1. System administration and elevated privilege user accounts shall be appropriately secured.

CF 5.3.2. Administrators and privilege users shall use basic user accounts for normal day-to-day activities such as e-mail and authorized Internet access with such usage prevented on their higher level accounts unless approved by management.

CF 5.3.3. Administrative and privilege user functions shall be approved by management and have individual account credentials to prevent compromise.

CF 5.3.4. Administration account functions shall be monitored, securely logged and independently audited within a segregation of duties and records maintained.

CF 5.3.5. System administration and elevated privilege user accounts shall be disabled prior to notification of termination.

CF 5.4. System Basic User Accounts

Summary: CF 5.4 sets out the requirements for system basic user accounts. The principle of least privilege must be adopted across the environment such that user account access, permissions to files, folders and systems is provided where a business need is identified. See CF 6 for training and awareness requirements.

Requirements:

CF 5.4.1. IT User accounts shall be appropriately secured.

CF 5.4.2. User accounts shall be disabled prior to notification of termination.

CF 5.4.3. User accounts shall be reviewed on a regular basis on the principle of least privilege and to ensure that unauthorized accounts do not remain active.

CF 5.5. Authentication Management

Summary: CF 5.5 sets out requirements for Authentication management. Authentication (using passwords or biometrics) is the front line of protection for user accounts and network access. Password rules must be in place to separate and define the complexity, length, use and re-use for system level and user passwords. Password controls provide actions for password lifecycle, reset requirements and actions to be taken on suspicion of password compromise.

Requirements:

CF 5.5.1. All IT users shall have individual user accounts controlled by username and password credentials or secure biometric authentication. Where used, different passwords shall be used for administrator, privileged and user accounts.

CF 5.5.2. Password format, history and complexity requirements must be established, set and monitored at administrator level.

CF 5.5.3. Password expiry time shall be defined.

CF 5.5.4. Users shall be responsible and accountable for their password security and quality.

CF 5.6. Authorizing Third-party Access to IT Systems

Summary: CF 5.6 sets out the requirements for controlling third-party access to IT systems with the aim of protecting confidential company and client data.

Requirements:

CF 5.6.1. Third party IT access shall be pre-authorized, documented, monitored and reviewed.

CF 5.6.2. Third-parties shall be required to adhere to the participants IT Security Policy and procedures.

CF 5.6. Authorizing Third-party Access to IT Systems

CF 5.6.3. The IT Security Policy shall be communicated to, and a record retained of the third party companies’ acceptance and individuals’ acceptance and understanding of the content.

CF 5.7. Removable Media

Summary: CF 5.7 sets out requirements for controlling removable media capable of read/writing original data from computers. Common examples are USB drives, external HDD, tablets, smart phone, etc and may be company or personal property. Such devices represents a significant threat to the loss or compromise of media assets.

See CF 4 for restriction on prohibiting personal devices within designated secure areas.

Requirements:

CF 5.7.1. Unauthorized or non-essential devices shall be prevented from accessing the network. Authorization criteria and a procedure shall be established. An asset register of authorized devices shall be maintained.

CF 5.7.2. Authorized devices shall be clearly identifiable using a permanent and unique solution.

CF 5.7.3. Procedures shall be aligned to an ‘’end point’’ security solution and network access controls.

CF 5.8. Mobile Device Management

Summary: CF 5.8 sets out the requirements for acceptable use of mobile devices capable of processing, transmitting or storing sensitive company data or client information away from the participant premises. Data in this context is defined as client assets in electronic form, sensitive company information, correspondence or records. Common examples of mobile devices include laptops, tablets and smart phones.

Requirements:

CF 5.8.1. Content assets shall not be stored on mobile devices unless:

- A risk assessment is completed.
- Management approval to do so has been given.
- The requirements of CF5.24 ‘Encryption and Key Management’ are complied with.

CF 5.8. Mobile Device Management

The participant shall maintain a secure inventory of mobile devices storing content assets.

CF 5.8.2. Mobile devices used for processing or storing client assets shall be authorized for introduction to and removal from the site by an IT system administrator.

CF 5.8.3. 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 5.8.4. All mobile devices used for processing or storing client assets shall be:

- Securely backed up on a regular basis to avoid loss of data
- Protected with:
  - Malware and firewall software
  - Cable locks when left unattended

CF 5.8.5. Mobile phones shall be PIN locked on timeout. Mobile devices shall be password protected on timeout. Where an incorrect PIN / password is entered 5 times consecutively, this shall cause the device to lockout.

CF 5.8.6. The participant shall have the ability to remotely lock, wipe or find devices when a device is reported stolen or lost.

CF 5.9. Wireless Networks

Summary: CF 5.9 sets out the requirements for wireless networks. Deployment of these wireless networks needs to be carefully considered to prevent the unauthorized disclosure of confidential company or client data.

Requirements:

CF 5.9.1. A procedure covering participant wireless networks shall be created and communicated to IT system users.

CF 5.9.2. No wireless access shall be allowed into production or replication networks.

CF 5.9.3. All wireless access shall be protected from unauthorized access.

CF 5.9.4. All wireless signals shall be protected from information interception. As a minimum, WPA2 shall be implemented between infrastructure and client.

CF 5.10. Incident Management

Summary: CF 5.10 sets out the requirements for incident management. Logical security incidents are a known threat within content protection security and must be managed in a methodical and consistent manner governed by a policy and procedure

Examples of information security incidents may include, loss of facilities, system malfunctions, policy non-compliance, physical security breaches, and uncontrolled system changes, malfunctions of hardware/software and access violations.

See also CF 7 Business Continuity and Disaster Recovery Planning

Requirements:

CF 5.10.1. Incident management procedures shall be implemented that cover initial and extended triage of IT security incidents.

CF 5.10.2. For cloud environments, the participant shall develop and maintain additional requirements for incident response and immediate notification to the client in the event of any unauthorized access to systems or content.

CF 5.10.3. Roles and responsibilities for dealing with IT security incidents shall be defined.

CF 5.11. Physical and Environmental Security Controls

Summary: CF 5.11 sets out the requirements for physical and environmental security controls. The data and logical media assets received, produced, transferred, stored or shared by a participant must be physically as well as logically protected. Ensuring the correct environmental controls are implemented is essential. The controls deployed at sever and data storage locations are dependent on the size and infrastructure of the business. Controls may include fire and heat sensors, fire suppression systems, intruder alarms, CCTV, secure rooms, electronic access control and procedural security controls.

Requirements:

CF 5.11.1. Participants shall establish adequate controls to physically protect and control access to network devices, servers, firewalls and data stores.

CF 5.11.2. Access shall only be given to authorized personnel based on a business need to routinely access, visit, or work in the designated secure area.

CF 5.11.3. Details of visitors to the secure locations shall be documented giving time date and purpose for the visit. All visitors shall be escorted.

CF 5.11.4. In the case of shared services the physical access to servers shall be secured using secured cabinets. Keys and combinations shall be issued and retained by an appointed administrator.

CF 5.11. Physical and Environmental Security Controls

CF 5.11.5. Data stores (especially backup stores) shall be protected from poor environmental conditions, which include dust, dirt, smoke and strong electromagnetic fields.

CF 5.11.6. Locations shall be inspected on a regular basis and subject to routine maintenance.

CF 5.12. IT Asset Management

Summary: CF 5.12 sets out the requirements for asset registration, use and disposal. A register of the physical and logical assets used to operate, control and protect IT systems, production and replication networks is to be maintained. Information identifying the asset location, date of deployment, system maintenance, updates, development and change management requirements assists to locate, protect and schedule any required changes.

Physical IT assets should be marked, referenced or have bar code registration. Software assets and applications would normally be registered using imaging software solutions combined with system management utilities for scheduling and/or approving security updates.

Removable media is defined as a device or media that is readable and/or writable by an end user and can be moved from computer to computer without modification and may include; USB storage device, external HDD, tablet pc, smart phone, etc. Removable media represents a significant threat to the loss or compromise of media assets. Such media may be owned/controlled by the organization or an individual.

The destruction or removal from use of all hardware and associated digital assets must be properly authorized, the methodology documented and destruction certificates retained to provide an auditable trail in the event of an incident.

See CF 4 for restrictions on prohibiting personal devices within designated secure areas. Checks and controls are necessary to protect the network and systems from un-authorized or malicious use of such devices. Additional risks may include the introduction of malware or viruses.

Requirements:

CF 5.12.1. Individual responsibilities and accountability for IT asset management shall be defined.

CF 5.12.2. All IT assets and software shall be subject to an acceptance and ‘authorization for use’ process approved by the Director with responsibility for IT.

CF 5.12.3. An IT Asset Register shall be maintained detailing all IT assets owned, or controlled by the organization. For cloud environments this shall include a complete inventory of all critical cloud IT assets, including ownership of the asset.

CF 5.12.4. 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 5.12. IT Asset Management

CF 5.12.5. 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 5.12.6. 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 5.12.7. Policy shall be aligned to an ’’end point’’ security solution and network access controls.

CF 5.12.8. 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 5.12.9. Hardware and associated devices identified as being redundant shall have all stored data sanitized prior to repair or disposal. Records of data sanitization and disposal shall be maintained.

CF 5.13. Network Monitoring

Summary: CF 5.13 sets out the requirements for monitoring network activity. System monitoring is important to detect unauthorized activities and any incidents investigated in line with CF5.10 Incident Management.

Requirements:

CF 5.13.1. The participant shall implement logging mechanisms on all systems handling or used for the following:

- Digital client assets(including network devices involved in the transmission of these assets)
- Key generation and management
- Vendor certificate management.

CF 5.13.2. The participant shall implement a process to:

- protect log information from deletion or change
- review logs regularly, and
- define a system to report findings and investigate anomalies.

CF 5.13. Network Monitoring

CF 5.13.3. The logs shall include information relating to events and changes to security hardware and software and provide enough detail to allow effective investigation.

CF 5.14. Access Controls

Summary: CF 5.14 sets out the requirements for authorizing and controlling user access to relevant IT systems. Oversight and control of access to information systems is important to mitigate the risk of loss or compromise to client data. Access controls can be both physical and logical (i.e., tools used to identify, authenticate or authorize users on computer systems).

Requirements:

CF 5.14.1. The participant shall establish and configure effective technologies to secure access to computer systems, network devices and confidential information (including content assets) based upon the principle of 'Least Privilege'.

CF 5.14.2. Authorization permissions should follow mandatory access control (MAC), discretionary access control (DAC) and or role-based access control (RBAC) principles. For project based activities, participants shall restrict user access to content on a per-project basis.

CF 5.14.3. Records of management authorization approval activities (e.g., approval emails, change request forms) shall be retained.

CF 5.14.4. Where possible on systems that handle content assets, local accounts shall be disabled or removed.

CF 5.14.5. Workstations shall be configured to lock out after a defined period of inactivity.

CF 5.14.6. Controls and access permissions to IT systems (including client web portals) shall be reviewed at least quarterly.

CF 5.15. Remote Access

Summary: CF 5.15 sets out the requirements for authorizing and accessing network systems from remote locations. As defined within 0, it is essential that participants have full knowledge and oversight of information systems accessed remotely. Remote access controls must be enforced to mitigate the risk of loss or compromise to client content. Access controls can be both physical and logical (i.e., tools used to identify, authenticate or authorize users on computer systems).

Requirements:

CF 5.15.1. Remote access to IT systems shall require prior management authorization based upon an identified business need.

CF 5.15.2. Participants 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 5.15.3. Where remote IT systems access is approved, connection via multi factor authorization VPN shall be required.

CF 5.15.4. Controls and remote access permissions should be reviewed regularly to ensure they continue to deliver the necessary security.

CF 5.16. Change Management

Summary: CF 5.16 sets out the requirements for ensuring that all system configuration changes are properly authorized, tested and implemented and is intended to ensure that changes may be made with minimized disruption to business operations.

Requirements:

CF 5.16.1. Change management processes shall ensure that all changes to IT systems (including cloud systems) undergo a formal prior impact assessment, formal review and approval from stakeholders. It should include a method for recording significant changes, planning and testing of changes and communication of changes to relevant persons.

CF 5.16.2. Fallback procedures must be documented to mitigate the risk of unsuccessful changes

CF 5.17. System Documentation

Summary: CF 5.17 sets out the requirements necessary to give management sight of the full IT System landscape. Clear and well-defined system architectural documentation allows immediate and easy reference to the network landscape. This evidences the security strategy of the business through diagrammatical representation. Such representation aligns with the overarching IT security policies.

Requirements:

CF 5.17.1. Participants shall ensure that their IT systems and networks (including cloud environments) are appropriately documented and mapped.

CF 5.17. System Documentation

CF 5.17.2. System documentation shall be treated as confidential and stored securely to prevent inappropriate exposure of possible vulnerabilities

CF 5.18. External Networks and Wide Area Networks

Summary: CF 5.18 sets out the requirements necessary for ensuring network integrity through segregation. External networks are those network segments with direct internet access such as DMZs (demilitarized zones). Because of their fringe status (i.e., housing public facing servers) they are inherently susceptible to attack and require special consideration in relation to security controls employed.

Requirements:

CF 5.18.1. Participants shall establish, document and implement baseline security requirements for WAN network infrastructure devices and services.

CF 5.18.2. All external content bearing network segments shall be monitored for anomalies.

CF 5.18.3. All external connections shall be recorded and assessed based against business requirements and reviewed regularly

CF 5.18.4. As a minimum participants shall perform:

- quarterly vulnerability scans, and
- annual penetration testing of all external IP ranges and hosts
- ….and remediate any issues discovered.

CF 5.19. Internal and Local Area Networks

Summary: CF 5.19 sets out the requirements necessary to ensure proper internal network segregation. Internal networks are those network segments with no direct internet access. There may be multiple internal segments dedicated to various functional areas such as production, HR, finance, etc.

Requirements:

CF 5.19.1. All internal content bearing network segments shall be mapped and secured from unauthorized access in line with CF5.14 Access Controls and CF5.15 Remote Access.

CF 5.19.2. All production, development and general network segments shall each be securely segregated.

CF 5.19. Internal and Local Area Networks

CF 5.19.3. Production segments shall have no direct connection to the Internet.

CF 5.19.4. All network segments transporting content shall be monitored for anomalies.

CF 5.19.5. Administration functions shall be adequately segregated to protect client assets.

CF 5.19.6. Externally accessible servers (e.g., web servers) shall be placed within the DMZ.

CF 5.20. File Transfer Management

Summary: CF 5.20 sets out the requirements relating to file transfer technologies and encryption of data. File transfer technologies in this context are those information exchange systems used by content owners to distribute media to their supply chains and end users for instance Aspera, Signiant, WAM Net, SmartJog and Secure File Transfer Protocol (SFTP). Encryption is often used where content is transferred by satellite, high-speed internet connection, and portable hard drives or where embedded in hardware (e.g., digital cinema package technology).

Requirements:

CF 5.20.1. Participants shall implement and use dedicated systems for content file transfers. These shall be placed in a DMZ and not in content/production networks.

CF 5.20.2. Transferred content shall be removed from the DMZ immediately after successful transmission/receipt

CF 5.20.3. Participants shall document:

- All connections from production networks used to transfer digital client assets
- A procedure for recording access to, or authorization for transfer of digital client's assets.

CF 5.20.4. Digital assets transferred or routed outside of a secure production network shall be client approved and follow the requirements of CF5.25 Encryption and Key Management.

CF 5.20.5. The system shall send automatic notifications to the production coordinator(s) upon outbound content transmission.

CF 5.20.6. Transmission of content using email (including webmail) from client portals shall be prohibited

CF 5.20.7. Where key delivery messages (KDMs) are used, they shall be time specific and valid only for a specific destination device.

CF 5.20. File Transfer Management

CF 5.20.8. Where relevant, production and hosting environments shall provide verification of the file integrity using hashed-based message authentication code (HMAC) or equivalent

CF 5.20.9. Participants shall establish internal audits of the transfer of digital client assets

CF 5.21. Firewall Management

Summary: CF 5.21 sets out the requirements for firewall management. Firewalls control traffic flow between a trusted network (e.g., corporate LAN) and an untrusted or public network (e.g., internet) and are essential to protect IT systems from external attack.

Requirements:

CF 5.21.1. All external connections shall be controlled through a firewall. Consideration should be given to also controlling connections to and from production networks through a firewall.

CF 5.21.2. Firewall technology and configurations used should be appropriately sophisticated and effective for the level of security required and be subject to regular management review. As a minimum firewalls shall be configured to deny all protocols by default and enable only specific permitted secure protocols to pass.

CF 5.21.3. Firewall rules shall be reviewed to confirm configuration settings are appropriate and required by the business every 6 months.

CF 5.21.4. Remote management of the firewall from any external interface(s) (including via a remote desktop connection) shall be prohibited.

CF 5.21.5. Security incidents detected by firewalls should be recorded and investigated. (See CF 5.10 Incident Management).

CF 5.21.6. Automatic alerts shall be sent to the systems administrator when a firewall configuration changes or re-boots and if necessary investigated

CF 5.22. Network Infrastructure and Configuration

Summary: CF 5.22 sets out the requirements for Network Infrastructure and Configuration

Requirements:

CF 5.22.1. Participants shall:

- Use appropriately secure configuration on networks
- Designate specific systems to be used for content input/output (I/O)
- Separate content transfer systems from administrative and production networks.

CF 5.22.2. The web portal shall be placed on a dedicated server in the DMZ and access to/from it limited to specific IP addresses and protocols/port numbers.

CF 5.22.3. The use of third-party production software/systems/services that are hosted on an internet web server shall be prohibited unless approved by client in advance.

CF 5.22.4. Access to content on internal or external portals shall be set to expire automatically at predefined intervals, where configurable.

CF 5.22.5. Participants shall:

- test for (client portal) web application vulnerabilities quarterly
- perform annual penetration testing of (client portal) web applications

- and remediate any validated issues.

CF 5.22.6. Only authorized personnel shall be allowed to request the establishment of a connection with the telecom service provider

CF 5.22.7. Network infrastructure devices, SAN/NAS, and servers shall be hardened based on security configuration standards.

CF 5.22.8. Backups of network infrastructure/SAN/NAS devices and servers shall be secured to a centrally secured server on the internal network.

CF 5.22.9. The participant shall implement a secure synchronized time service protocol (e.g., Network Time Protocol v3 or above) to ensure all systems have a common time reference. Authentication between the client and the time source server should be enabled

CF 5.22.10. The participant shall conduct internal network vulnerability scans and remediate any issues, at least annually.

CF 5.22.11. For cloud environments, the participant shall:

- Ensure procedures prevent non-production data being replicated to production environments
- Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections

CF 5.22. Network Infrastructure and Configuration

- Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/from virtual servers.

CF 5.22.12. For cloud and virtual environments the participant shall ensure client content and data is appropriately segmented within multi-tenant applications, systems, and components.

CF 5.23. Vulnerability Management

Summary: CF 5.23 sets out the requirements necessary for vulnerability management including anti-virus protection, security updates (patches) system and data backups and security testing. Threats to IT systems such as malware or internal vulnerability exploitation can be mitigated by applying a regime of good housekeeping. If not protected and updated, systems can become unstable, causing loss of data. Failure to back data up can make this loss permanent and compromise client assets.

Requirements:

CF 5.23.1. All servers, workstations and mobile devices shall be protected from malicious software (malware/viruses). Exceptions to deployment of such protection shall be documented and justified, and alternative methods for protection must be defined.

CF 5.23.2. Anti-virus software shall be updated at least weekly on workstations and mobile devices, and daily on servers

CF 5.23.3. Anti-virus solutions shall not be capable of being disabled by basic users

CF 5.23.4. Anti-virus shall perform on access scanning and scheduled background scanning at least monthly on workstations and weekly on servers.

CF 5.23.5. Anti-virus shall, as minimum, quarantine suspicious files.

CF 5.23.6. All servers, workstations and mobile devices shall have software updates (patches) updated at least monthly; security barriers shall be patched at least weekly.

CF 5.23.7. All justifications for non-patching must be documented, justified and where appropriate alternative mitigating controls implemented, for example where manufacturer software support is no longer available.

CF 5.23.8. 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 5.23.9. Public facing servers shall not have any internal facing credentials stored. Internal facing servers shall not have access to the internet.

CF 5.23. Vulnerability Management

CF 5.23.10. The participant shall provide evidence of vulnerability assessment and shall consider an appropriate level of testing to be applied according to documented risk assessment.

CF 5.24. Encryption and Key Management

Summary: CF 5.24 sets out the requirements for encryption of data and content assets at rest and in motion.

Requirements:

CF 5.24.1. Unless a business critical application prevents doing so client data and content assets shall be encrypted at rest and in motion, including across virtual server instances, using AES 128-bit as a minimum. Encryption may be file based or drive based. For mobile devices this requirement will always apply, at least for areas of the device where content assets will be handled or stored.

CF 5.24.2. Secret and private keys (but not public keys) used to encrypt data/content shall be appropriately secured.

CF 5.24.3. Decryption keys or passwords shall be transported or transferred using an out-of-band communication protocol (i.e., not on the same transmission method or storage media as the content itself).

CF 5.24.4. The participant shall Implement and document key management procedures.

CF 5.24.5. For cloud environments appropriate additional key management features, controls, policies and procedures shall be documented and implemented. Encryption keys shall not be stored in cloud environments.

CF 6. TRAINING AND AWARENESS

CF 6.1. Training and Awareness Needs

Summary: CF 6.1 sets out the requirements for the training and awareness needs relating to security. All employees, contractors, consultants and third-parties must be trained to deliver their services securely and are made aware of the security measures and requirements on the site to protect the confidentiality and integrity of customer assets and intellectual property. The provision of an established policy ensures management commitment and adequate budget.

Requirements:

CF 6.1.1. 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.

CF 6.1.2. Security training and awareness shall be planned and delivered as required according to role and responsibility.

CF 6.1.3. 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 6.1.4. Specific security requirements of the CPS Standard, legal, regulatory and contractual obligations shall be identified, reviewed and incorporated into the training program. IT Users must be aware of participants IT security policies and procedures relevant to their role.

CF 6.1.5. The participant shall ensure that records of attendance are maintained. Records shall include details of training package content, name of the instructor, and dates of training and results of any examinations or assessments.

CF 6.1.6. 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.

CF 6.2. Dedicated and Skilled IT Security Staff

Summary: CF 6.2 sets out the requirement for dedicated and/or skilled IT security staff. A single and dedicated IT security role may not be practicable within every organization. However, irrespective of size or operation the risks to digital media assets must be mitigated. Participants must ensure, as a minimum, that IT administrators are sufficiently aware of IT security related threats and vulnerabilities. In certain cases the adoption of dedicated security functions is necessary and must be considered as part of the risk management process.

Requirements:

CF 6.2.1. The participant shall provide IT security training to support administrative functions.

CF 6.2.2. The participant shall have independent managerial oversight of the operations of the network support team and should consider an IT security role independent of the network support team.

CF 6.3. Personnel Participation

Summary: CF 6.3 sets out the requirement to provide a mechanism for staff involvement in developing a positive security culture within the organization. Ownership of security policies by staff can help improve security or resolve issues not previously identified by management. The ability to report matters such as security incidents, breaches or non-compliances anonymously and without fear of retribution can greatly enhance the overall security culture of an organization and reduce the risk of loss or compromise. Basic systems such as a suggestions box or confidential hotlines can prove effective communication and convey a message of commitment and engagement.

Requirements:

CF 6.3.1. 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 6.3.2. Management shall provide methods for employees to report security issues without fear of retribution.

CF 7. Business Resilience

CF 7.1. Business Continuity Planning (BCP)

Summary: CF 7.1 sets out the requirements for business continuity planning (BCP). BCP is the management process to ensure continued operations if an incident occurs. DRP is the recovery process to restore normal operations. The participant is required to define the roles, responsibilities and plans for BCP. The management process and recovery plan must be commensurate to the organization’s size, geographical location and services provided. Events to be considered include but are not exclusive to natural disaster, fire, flood, accident, pandemic, civil unrest, equipment failures and deliberate or malicious acts of sabotage.

Requirements:

CF 7.1.1. A Business Resilience (BR) Team shall be established.

CF 7.1.2. A Business Impact Analysis (BIA) and Risk Assessment should be conducted to identify key products and services; the critical activities needed to support these; the impact that a disruption of these activities would have on your organization and the resources needed to restore business operations.

CF 7.1.3. Maximum Tolerable Periods of Disruption (MPTD) and Recovery Time Objectives (RTO) should be recorded within the BIA.

CF 7.1.4. Quantify resources required to meet RTO.

CF 7.1.5. A BR Plan shall be published and communicated to the BR Team and key employees where necessary.

CF 7.1.6. At least annually the participant shall complete:

- Effective testing of the BR plan
- A management review of this plan

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

CF 7.2. Disaster Recovery Planning (DRP)

Summary: CF 7.2 sets out the requirements for Disaster Recovery Planning (DRP). A DRP should be developed in conjunction with the Business Continuity Plan. Priorities and recovery time objectives for information technology should be developed during the Business Impact Analysis. The participant is required to define the roles,

CF 7.2. Disaster Recovery Planning (DRP)

responsibilities and plans for DRP. The management process and recovery plan must be commensurate to the organization’s size, geographical location and services provided.

Requirements:

CF 7.2.1. Business impact assessment based recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

CF 7.2.2. Effective IT Asset management (See CF 5.12) will assist with identification of critical software applications and hardware.

CF 7.2.3. Internal or Vendor Supported recovery strategies should consider data back-ups or mirroring so that data can be restored.

CF 7.2.4. A DR Plan shall be published and communicated to the BR Team and key employees where necessary.

CF 7.2.5. At least annually the participant shall complete:

- Effective testing of the DR plan
- A management review of this plan

CF 7.2.6. Participants shall document findings of reviews and tests, and update the DR plan accordingly.

CF 7.3. UPS and Maintenance

Summary: CF 7.3 sets out the requirements for ensuring that security systems are suitably maintained and are provided with a continuous power source.

Requirements:

CF 7.3.1. Uninterrupted power supplies (UPS) must extend to all security systems and sized appropriately for local conditions and business activities.

CF 7.3. UPS and Maintenance

CF 7.3.2. Security systems shall be maintained and tested in accordance with manufacturer’s guidelines. Where third-parties are used, requirements set out in CF 2.2 shall be followed.

CF 7.4. Evacuation Procedures

Summary: CF 7.4 sets out the requirements for establishing, testing and reviewing evacuation plans.

Requirements:

CF 7.4.1. An evacuation plan shall be published and communicated

CF 7.4.2. Evacuation procedures shall take account of maintaining the security of the site and protecting content assets, subject to local laws and regulations.

CF 7.4.3. At least annually the participant shall complete:

- Effective testing of the evacuation plan
- A management review of this plan

CF 7.4.4. Participants shall document findings of reviews and tests, and update the evacuation plan accordingly.