



Anti-Piracy & Compliance Programs



Content Protection and Security Standard



Revised January 21, 2011

Requirements for Accreditation

With knowledge and experience working within the supply chain, CDSA has identified the need for a more granular yet practical approach to effective site security. To achieve this, CDSA has developed a series of “requirements” within each of seven Fields of Capabilities.

The determination of inherent risk levels Schedule of Requirements forms the backbone of the accreditation process. The requirements shall be reviewed and amended as necessary. This list may expand and adjust organically as the framework, available technologies and process requirements change, thus forming part of CDSA’s policy review, its risk assessment and in support of its accreditation.

Based upon the capability framework the Standard sets out how each site shall identify the relevance of each control to their organization and develop selected controls or justify reasons for not implementing controls in a Statement of Applicability.

By completing the Statement of Applicability (SoA) each site shall demonstrate its capability to meet the mandatory operational security management system requirements. Site capabilities will be assessed by CDSA during an on-site audit for the site to attain accreditation. CDSA will accredit the site, if either zero non-compliances or one or more non-systemic (minor) non-compliances are observed. Sites where one or more major or systemic noncompliance(s) are observed will fail to receive accreditation until the issues are addressed adequately, and re-assessed onsite by CDSA.

Declination of Liability

CDSA has made every effort to formulate a standard that it believes will help manufacturers 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 shall decline any liability toward a content owner, manufacturer, 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	4
CF 1.1	Documentation	4
CF 1.2	Risk Management	5
CF 1.3	Compliance	6
CF 2	PERSONNEL AND RESOURCES	8
CF 2.1	Personnel	8
CF 2.2	Resources.....	9
CF 3	ASSET MANAGEMENT	10
CF 3.1	Responsibilities and Authorities	10
CF 3.2	Asset Receipt and Identification	11
CF 3.3	Asset Inventory and Traceability	12
CF 3.4	On-site Asset Handling	13
CF 3.5	Asset Storage	14
CF 3.6	Transport of Out-going Assets	15
CF 3.7	Destruction and Recycling of Assets	16
CF 3.8	Asset Tracking Records	17
CF 4	PHYSICAL SECURITY	18
CF 4.1	Physical Security Plan	18
CF 4.2	Layered Physical Security Measures	19
CF 4.3	Securing the Site Perimeter	20
CF 4.4	Securing Internal Areas	21
CF 5	IT AND ELECTRONIC DATA SECURITY	22
CF 5.1	High Level Security Measures	22
CF 5.2	Personnel Security Vetting	25
CF 5.3	Acceptable Security	26
CF 5.4	Infrastructure Security Measures	31
CF 5.5	Personnel Training	35
CF 5.6	Additional Requirements for Digital Operations	37
CF 6	TRAINING AND AWARENESS	44
CF 6.1	Defined Training and Awareness Needs.....	44
CF 6.2	Provision of Training	45
CF 6.3	Personnel Understanding of Security Management System	46
CF 6.4	Training Records.....	47
CF 6.5	Provision of On-going Security Management System Awareness	48
CF 6.6	Avenues for Personnel Participation in Security Management System.....	49
CF 7	DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING	50
CF 7.1	Recovery and Continuity Plans	50
CF 7.2	DRP/BCP	51

CF 1 DOCUMENTATION, RISK MANAGEMENT AND COMPLIANCE

CF 1.1 Documentation

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

CF 1.1.1.1 approving documents prior to use,

CF 1.1.1.2 ensuring that document changes and current revisions of documents are properly identified through an appropriate means,

CF 1.1.1.3 reviewing and updating documents when needed,

CF 1.1.1.4 ensuring documents are legible, identifiable, and properly stored and maintained,

CF 1.1.1.5 ensuring current document are available where needed, and

CF 1.1.1.6 preventing the 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

CF 1.2.1 Risk management is a systematic process for identifying, analyzing, and treating (mitigating) risks to assets. When implementing risk management, the site shall consider the nature of its operations, including its inherent risks to asset security, related legal and regulatory environment, as well as business and customer requirements.

CF 1.2.2 Responsibilities and authorities for risk management process shall be defined by management. Management also shall define, implement and maintain risk management processes, which include methods for:

CF 1.2.2.1 risk assessment: the identification of risks, including what assets may be impacted and how,

CF 1.2.2.2 analysis and evaluation of risks: the review of existing security risks and the existing security controls to determine the likelihood of a threat or loss of an asset, and the related consequences to determine a risk level,

CF 1.2.2.3 Statement of Applicability and risk mitigation: the resulting decision to accept, or treat risk with security control measures (policies, procedures, technology, etc.). The decision is typically based upon the scope of operations, available resources, risk exposure levels and their possible impact, and priorities. The site shall document a Statement of Applicability which summarizes the capabilities that shall be implemented, and any exclusions from the security management system, and

CF 1.2.2.4 recording outcomes.

CF 1.2.3 Management shall take steps to monitor and evaluate the security management system, its policies and control measures to ensure its on-going effectiveness. When operational changes affecting asset security arise, the Statement of Applicability (SoA), policies and procedures shall be reviewed, modified or revised to address needs, as needed. Changes shall be recorded.

CF 1.3 Compliance

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:

- CF 1.3.1.1 security incident monitoring and response,
- CF 1.3.1.2 corrective and preventive actions,
- CF 1.3.1.3 internal audits,
- CF 1.3.1.4 external CDSA audits, and
- CF 1.3.1.5 management review of security management system performance.

CF 1.3.2 The site shall establish, implement and maintain a security incident monitoring and response process to monitor, detect, and respond in a timely manner to security incidents and characteristics of its activities that can have a significant negative impact on content security. A procedure(s) shall address methods for.

- CF 1.3.2.1 identifying the type of security incident (e.g., theft, premature release, or loss of intellectual property and related media or assets, etc.),
- CF 1.3.2.2 gathering details about the security incident (e.g., the nature of the incident, date, time and location of incident, and those involved in the incident),
- CF 1.3.2.3 investigating security incidents and their root causes,
- CF 1.3.2.4 characterizing the significance and impact of the actual or potential loss,
- CF 1.3.2.5 initiating immediate corrective action and/or preventive action as necessary, and
- CF 1.3.2.6 evaluating the effectiveness of any actions taken to address security incidents.

The site shall maintain and retain associated records for at least 3 years.

CF 1.3.3 Corrective and preventive action processes shall:

- CF 1.3.3.1 effectively eliminate the root causes of actual non-compliances and prevent their reoccurrence,
- CF 1.3.3.2 effectively eliminate the potential of unauthorized release/access to content and system non-conformities, and prevent their reoccurrence,
- CF 1.3.3.3 ensure actions are effectively implemented in a timely fashion,
- CF 1.3.3.4 ensure actions taken are commensurate to the potential risks encountered, and the effects on content security, and
- CF 1.3.3.5 address non-compliances, internal and external audit results.

The site shall maintain and retain associated records for at least 3 years.

CF 1.3.4 Internal audit procedures shall ensure:

- CF 1.3.4.1 operations comply with requirements, and that the program is sufficiently implemented and maintained to effectively protect assets,
- CF 1.3.4.2 internal audits are scheduled and performed at least once per year,
- CF 1.3.4.3 personnel independent of those having direct responsibility for the activity being audited carry out such audits,
- CF 1.3.4.4 results of the internal audits are recorded and reported to personnel having responsibility in the areas audited for appropriate corrective or preventive action in a timely manner,
- CF 1.3.4.5 follow-up activities verify and record the implementation and effectiveness of corrective actions, and
- CF 1.3.4.6 results of internal audits, and related corrective and preventive actions are

CF 1.3 Compliance

included in management review.

CF 1.3.5 Upon initial CDSA Content Protection and Security audit, if successful, the site shall be accredited for a 6 month period. If one or more minor non-compliances are found in this audit, the facility shall have 30 days to submit a corrective action report to the CDSA auditor. If one or more major (or systemic) non-compliances are found, the site shall not receive accreditation until it implements effective corrective action within 30 days, and completes a CDSA re-audit.

Following the initial 6 month accreditation period, a further external CDSA Audit shall be carried out, and, if successful, the site shall be accredited for a 12 month period. The site shall then undergo external CDSA Audits for CDSA Content Protection and Security Accreditation on an annual basis. If one or more minor non-compliances are found in these audits, the facility shall have 30 days to submit a corrective action report to the CDSA auditor. If one or more major non-compliances revealed by an internal or external audit are not corrected, documented to CDSA, and re-audited within 30 days of discovery, CDSA reserves the right to suspend accreditation until appropriate corrective actions are implemented and, at CDSA's option, publicly acknowledge such suspension.

CF 1.3.6 Management shall review system performance at specified intervals to ensure its continuing suitability and effectiveness. This review shall include the results of ongoing risk management activities, security incident monitoring, corrective and preventive action, internal and external audits, review of policies and procedures, and identify improvement opportunities plans and required resources. Management review records shall be documented and maintained.

CF 2 PERSONNEL AND RESOURCES

CF 2.1 Personnel

CF 2.1.1 Management shall appoint a security management system 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:

CF 2.1.3.1 recruiting and hiring practices,

CF 2.1.3.2 new hire background or other checks,

CF 2.1.3.3 confidentiality agreements,

CF 2.1.3.4 job changes and reassignments,

CF 2.1.3.5 disciplinary actions against personnel, and

CF 2.1.3.6 personnel termination practices.

CF 2.1.4 When there are job changes, reassignments, and personnel terminations, management shall take appropriate action to make appropriate arrangements, including:

CF 2.1.4.1 asset and knowledge transfer, when applicable, and

CF 2.1.4.2 reassignment and/or removal of access; access rights minimize security risks, and ensure continuity of process functions.

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

Management shall identify and ensure the availability of finance and other resources for security management to adequately manage security risks, meet service level agreements and other contractual obligations, and identify opportunities to improve.

Management shall review the security management system performance to monitor, analyze, implement and improve processes to ensure media/content confidentiality, integrity, availability, and retrieval. Such reviews consider the results of audits, security monitoring and incident response, and other indicators of security management system performance and effectiveness.

CF 2.2 Resources

- CF 2.2.1 Management shall identify and ensure the availability of adequate budget allocation for needed for security management and to adequately manage security risks, meet service level agreements and other contractual obligations, and identify opportunities to improve.
- CF 2.2.2 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 2.2.3 Management shall review the security management system performance to monitor, analyze, implement and improve processes to ensure media/content confidentiality, integrity, availability, and retrieval. Such reviews consider the results of audits, security monitoring and incident response, and other indicators of security management system performance and effectiveness.

CF 3 ASSET MANAGEMENT

CF 3.1 Responsibilities and Authorities

Management shall define the responsibility and authority for asset management during its receipt, identification, handling, work in process, tracking, storage, disposition, destruction, labelling, packaging and transport.

CF 3.2 Asset Receipt and Identification

The site shall establish, implement and maintain processes to uniquely identify, log-in, and transfer assets from the point of receipt. At a minimum, the assets and products shall include customer-supplied master data sources, stampers, finished products and packaging material designed to prove product legitimacy (e.g. hologram stickers and authenticity stickers).

CF 3.3 Asset Inventory and Traceability

CF 3.3.1 The site shall establish, implement and maintain processes for asset inventory and traceability of all products to which the security framework applies.

Assets maintained for longer-term storage, including product samples, (i.e., not work in process) shall be maintained in an inventory control system. The types of assets (raw media, work in process media, final product, devices, etc.) included in the inventory control system shall be defined. Excluded assets shall be sufficiently justified. The inventory system shall have the ability to track the name of requester, the date, the asset location and its movement into and out of the designated storage areas.

CF 3.3.2 The site shall perform periodic cycle counts to count assets, confirm asset location, and assure the accuracy of inventory records.

CF 3.3.3 A process to reconcile the inventory, correct and address the root cause of any discrepancies shall be in place. This policy shall include a policy to inform the customer if a customer supplied asset is indeed missing. The organization shall also have policies to respond to cases of actual or potential theft or loss of assets (see also CF 1.1 section). Where applicable, finished products shall also be reconciled to inventory records.

CF 3.3.4 Inventory records shall be maintained for a minimum of 12 months.

CF 3.4 On-site Asset Handling

- CF 3.4.1 The site shall establish, implement and maintain policies and processes for supervising asset and equipment delivery and/or load-in/load out processes, accessing, identifying/labeling, logging, and transferring assets throughout each process from receipt to eventual removal, destruction, movement, transport, return to originator, and/or removal from the site's secure perimeter.
- CF 3.4.2 Access to work stations or production areas where assets are present shall be suitably monitored and controlled to prevent unauthorized access, asset theft or other losses. Methods shall be appropriate to the asset type and the risks posed.
- CF 3.4.3 Work in process assets shall not be left unattended or in an insecure location.
- CF 3.4.4 Vendors, subcontractors, transporters, and couriers shall be vetted to ensure that reasonable security measures are in place to protect assets, unless the customer specifies such parties, or the organization is reasonably certain of their reliability and the effectiveness of its security measures.
- CF 3.4.5 Suitable Service Level Agreements (SLAs), or equivalent, shall be executed by all such vendors, subcontractors, transporters, and couriers selected by the organization.

CF 3.5 Asset Storage

CF 3.5.1 When not in use, an asset shall be stored in a single locked storage location, which is restricted using suitable means to only authorized persons as authorized by management. Assets shall be stored in a secure location (e.g., locked vaults, libraries, SFTP sites, etc.) within the site's security perimeter.

CF 3.5.2 The storage location shall specify appropriate access controls and related devices (e.g., locks, key card access, magnetic badges, passwords, codes, etc.), environment/climate controls, including intrusion alarms, humidity and temperature controls, fire detection and fire suppression devices to secure and protect the integrity of assets.

CF 3.5.3 Management shall define policies for accessing storage locations. Access to storage location is restricted to only authorized persons, as determined by management. Entry to such storage locations shall be logged and monitored. Access control methods shall be appropriate to the type of asset, its value, its format, and its associated risks.

CF 3.6 Transport of Out-going Assets

Management shall establish, implement and maintain policies to authorize transport of outgoing assets. When assets are transported via mail or other package delivery service, certified mail or other tracking methods shall be used.

CF 3.7 Destruction and Recycling of Assets

Management shall establish, implement and maintain policies to authorize the destruction or recycling of obsolete, rejected or redundant assets and their media (e.g., rough cuts, masters, film, CD, DVD, DLTs, etc.). Methods shall ensure that such assets are unusable and cannot be copied. Records of asset receipt, movement or transfers on and offsite (including to/from personnel customers, vendors, service providers, etc.), as well as asset disposal, disposition, and returns shall be maintained for 12 months. Final disposition records shall also be kept for destroyed, recycled, or scrapped assets.

CF 3.8 Asset Tracking Records

Asset chain of custody records shall be kept when assets are transported to vendors, or other services providers (e.g., editing studios, authoring houses, manufacturing, packaging operations, etc.), customers and/or their agents, and site personnel.

CF 4 PHYSICAL SECURITY

CF 4.1 Physical Security Plan

CF 4.1.1 The site shall develop a Physical Security Plan. This plan demonstrates an ability to prevent, detect, mitigate and respond to a breach or attempted breach of the perimeter, the internal secure areas and locations where assets are stored.

CF 4.1.2 The plan shall include policies for controlling the:

CF 4.1.2.1 site security measures, including site access and authorization,

CF 4.1.2.2 site environment,

CF 4.1.2.3 site monitoring and management, and

CF 4.1.2.4 response to environmental threats or unauthorized attempts to access assets, including response to theft detected by video surveillance or searches.

CF 4.2 Layered Physical Security Measures

- CF 4.2.1 The site shall establish, implement and maintain policies for monitoring and controlling access to the security perimeter.
- CF 4.2.2 The site shall establish, implement and maintain policies for monitoring and controlling interior secure locations, including production and work areas.
- CF 4.2.3 The site shall establish, implement and maintain policies for monitoring and controlling asset storage locations.
- CF 4.2.4 The site shall establish, implement and maintain policies for monitoring and controlling, receiving and transport or shipping areas
- CF 4.2.5 There shall be a process for allowing, logging, limiting, monitoring and revoking access to the site, building, work areas, receiving and asset transport areas.
- CF 4.2.6 There shall be a process for staff, visitor, contractor, maintenance personnel and other third parties' searches. This process shall be proportional to the number of staff and visitors on-site and carried out on a percentage basis.

CF 4.3 Securing the Site Perimeter

The site shall demonstrate its capability to secure the defined physical site perimeter to cover all access points and the areas where assets are stored. The methods shall meet business needs. The organization shall specify and implement its on-site security measures to protect assets and may include one or more of the following:

- CF 4.3.1 Security guards, where used, may be either company staff or third party contractors. The site's Security Manual shall contain clear policies and procedures regarding guards and their duties.
- CF 4.3.2 Staffed reception areas during and after work hours.
- CF 4.3.3 Intruder detection systems (e.g., motion detectors, heat detectors, humidity detectors, glass break, PIR and/or movement detectors, other alarm system) with appropriate-range sensors, to cover all entrances/exits, and/or the areas where assets are stored. Intrusion detection systems shall: 1.) be monitored continuously, 2.) be connected to a dedicated line, 3.) have PIR and/or movement sensors; and 4.) log its activation and deactivation.
- CF 4.3.4 Secure entry gates and/or fences.
- CF 4.3.5 Walls, including rated fire walls.
- CF 4.3.6 Badges, and/or card key access.
- CF 4.3.7 Closed circuit television (CCTV), located to protect entrances/exits, production areas and areas where assets are stored. Such CCTV systems shall ensure appropriate zone coverage and image resolution.
- CF 4.3.8 CCTV systems and images/footage are stored securely. CCTV footage shall be maintained for a minimum of 90 days.
- CF 4.3.9 Access to the CCTV system is restricted to only security personnel or senior management, and/or other alternative personnel as appropriate.
- CF 4.3.10 There shall be a maintenance program in place to for all systems (e.g. intruder detection, CCTV, card access systems, monitoring systems etc.)
- CF 4.3.11 The site shall have processes for ensuring secured area access control to register and monitor staff, and third parties, including visitors, contractors and maintenance personnel.

CF 4.4 Securing Internal Areas

CF 4.4.1 The site shall secure and monitor the building(s), and internal areas containing content media or related assets, including vaults, safes, libraries, recording, mastering and mixing studios, control rooms, production areas, and data centers, as applicable. Such secure areas shall be identified.

CF 4.4.2 Security controls shall include:

CF 4.4.2.1 low visibility and secure areas, where possible, and

CF 4.4.2.2 entry controls limiting access into secured area to only authorized personnel.

CF 4.4.3 Access control measures that address:

CF 4.4.3.1 staff access control,

CF 4.4.3.2 visitor registration and access control,

CF 4.4.3.3 contractor and maintenance personnel registration and access control,

CF 4.4.3.4 other third-party access control,

CF 4.4.3.5 monitoring of secure areas access, and

CF 4.4.3.6 closed door policy to prevent unauthorized access.

CF 4.4.4 The site shall be capable of effectively monitoring, preventing, detecting and mitigating risks relating to a variety of threats, including theft, fire, water, power failures, vibration, vandalism, environmental threats, and other natural or manmade disasters.

CF 4.4.5 The use of equipment and other devices (e.g., fire/smoke detectors, vibration detectors, humidity detectors, uninterruptible power supply (UPS), etc.] to monitor and control the secure environment.

CF 5 IT AND ELECTRONIC DATA SECURITY

CF 5.1 High Level Security Measures

CF 5.1.1 Physical Security of Servers and Data Stores

CF 5.1.1 Physical Security of Servers and Data Stores

CF 5.1.1 Servers and data stores shall be protected from unauthorized physical access or attack, where servers and data stores can consist of any of the following:

- online Just-a-Bunch-of-Drives (JBOD) stores,
- online Network Attached Storage (NAS),
- online Storage Area Networks (SANs),
- offline backup devices and media (e.g., hard drives, DVD or CD stores, etc.), or
- offline backup tapes.

In all cases the following principles shall apply to data:

- CF 5.1.1.1 online data shall be physically secure,
- CF 5.1.1.2 data stores shall be protected from theft,
- CF 5.1.1.3 data stores (especially backup stores) shall be protected from poor environmental conditions, which include dust, dirt, smoke, strong electromagnetic fields, and strong magnetic fields.

Where the following requirements shall be undertaken:

- CF 5.1.1.4 physical access to servers shall be controlled and limited to only the authorized personnel with a need to access, visit or work in their location,
- CF 5.1.1.5 only authorized administrators are to have routine access to servers,
- CF 5.1.1.6 security personnel may have access to conduct reviews, log analysis or incident response activities,
- CF 5.1.1.7 other personnel are only to have access in exceptional circumstances, and
- CF 5.1.1.8 all visitors to the server room/area/cabinet are to be logged together with their access times and purpose of visit.

Physical access to servers is to be strictly controlled. However, where server facilities are shared, then the servers are to be in lockable cabinets. Care is to be taken to ensure that panels are not left insecure and that inter-rack paneling is installed.

The following are general security requirements that apply to all physical aspects of the system, servers, backup devices, backup media and any other aspect of the system that is held under lock and key or combination locks:

- CF 5.1.1.9 all lockable units shall be routinely locked irrespective of whether the area is occupied by personnel,
- CF 5.1.1.10 spare keys shall be correctly secured with policies regarding who can request use of the spare keys,
- CF 5.1.1.11 spare keys shall be swapped for the in-use keys every six months to prevent uneven wear in the keyset,
- CF 5.1.1.12 combinations shall be changed regularly and when any member of staff that knew the combination no longer has a need to know it or leaves the organization,
- CF 5.1.1.13 combinations shall be stored in a safe location,
- CF 5.1.1.14 combinations shall be sealed in an envelope by the person that sets the combination at the time they set the combination, and
- CF 5.1.1.15 combinations shall be stored in a fireproof and water resistant safe.

The site's Disaster Recovery Plan or Business Continuity Plan (DRP or BCP, see section CF 7)

CF 5.1.1 Physical Security of Servers and Data Stores

shall take into account accessing stored combinations and keys.

All records related to server and data store security and access are to be retained for a minimum of one year.

CF 5.2 Personnel Security Vetting

CF 5.2.1 Vetting System Administrators

CF 5.2.1 The site shall conduct background checks of system administrators and any personnel with high-level access to IT systems and data. The following are requirements for background checks:

- CF 5.2.1.1 the individual shall consent to supply the information for this purpose, and evidence of this consent shall be retained,
- CF 5.2.1.2 the individual's identity is validated,
- CF 5.2.1.3 the individual's birth place is confirmed,
- CF 5.2.1.4 two forms of identification, at least one with a photo, if possible,
- CF 5.2.1.5 the individual's last three claimed previous employers,
- CF 5.2.1.6 the individual's status with the last three previous employers,
- CF 5.2.1.7 the manner of departure from the last 3 previous employers,
- CF 5.2.1.8 verify claimed certifications with the issuing authority,
- CF 5.2.1.9 where public records are available, check the validity and expiry of the certifications,
- CF 5.2.1.10 check claimed qualifications where expedient,
- CF 5.2.1.11 verify qualifications achieved in the last 10 years, and
- CF 5.2.1.12 contact educational establishments to verify higher qualifications and degrees.

CF 5.3 Acceptable Security

CF 5.3.1 User Accounts

CF 5.3.1 The site shall establish, implement and maintain a User Account Policy (or a clause in an overarching Acceptable Use Policy).

CF 5.3.1.1 Users shall have individual user accounts and not share user accounts.

CF 5.3.1.2 Basic user accounts shall be configured to prohibit users from:

- installing software,
- uninstalling software,
- modifying any security software (e.g., anti-virus, firewall, HIDS, 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 privileges.

CF 5.3.1.3 The User Account Policy shall include methods to:

- convey the content of the policy to system administrators, and
- ensure each system administrator of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.3.2 System Administrator Accounts

CF 5.3.2 System Administrator Accounts

CF 5.3.2 The site shall establish, implement and maintain a System Administrator Account Policy (or a clause in an overarching Acceptable Use Policy).

System administrator accounts shall be configured and used according to the following:

- CF 5.3.2.1 no e-mail account shall be associated with an administrator account, which may be subject to cross-site scripting, phishing and cross-browser request forgery attacks,
- CF 5.3.2.2 administrators shall use basic accounts for day-to-day activities to prevent malware gaining cached credentials from administrator accounts,
- CF 5.3.2.3 administrators shall not use their privileged, higher level accounts to access the internet,
- CF 5.3.2.4 administrators shall not visit any external website whilst logged into the system with admin/system/root level privileges,
- CF 5.3.2.5 administrators shall have individual administrator accounts and not share an account,
- CF 5.3.2.6 on Unix systems, all users shall logon with regular accounts and SU to root, and
- CF 5.3.2.7 on Windows-based systems, administrators are to use lower non-administrator accounts for all normal user activity.

The System Administrator Account Policy shall include methods to:

- CF 5.3.2.8 convey the content of the policy to system administrators, and
- CF 5.3.2.9 ensure each system administrator of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.3.3 E-mail

CF 5.3.3 E-mail

CF 5.3.3 The site shall establish, implement and maintain an E-mail Policy (or a clause in an overarching Acceptable Use Policy).

The following shall be articulated so the user is fully aware of their responsibilities and liabilities with regard to:

- CF 5.3.3.1 users' accountability for their own actions when sending e-mail,
- CF 5.3.3.2 unless a user reports their account compromised, all e-mails are deemed to be sent by them,
- CF 5.3.3.3 the organization is required to protect its users from inappropriate e-mails,
- CF 5.3.3.4 definition of what constitutes an inappropriate e-mail,
- CF 5.3.3.5 highlight what actions the organization undertakes to stop inappropriate e-mails,
- CF 5.3.3.6 inform a user what they shall do if they receive an inappropriate e-mail,
- CF 5.3.3.7 direction from management should staff receive an inappropriate e-mail,
- CF 5.3.3.8 outline consequences to a user that sends inappropriate e-mail (either internally or externally),
- CF 5.3.3.9 appropriate style of e-mail language, and
- CF 5.3.3.10 the types of documents/attachments that can be sent.

The E-mail Policy shall include methods to:

- CF 5.3.3.11 convey the content of the policy to employees and e-mail users, and
- CF 5.3.3.12 ensure each employee and user of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

The E-mail Policy shall include methods to:

- CF 5.3.3.13 convey the content of the policy to users, and
- CF 5.3.3.14 ensure each user of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.3.4 Internet

CF 5.3.4 The site shall establish, implement and maintain an Internet Policy (or a clause in an overarching Acceptable Use Policy).

The following shall be articulated so the user is fully aware of their responsibilities and liabilities with regard to:

- CF 5.3.4.1 appropriate and inappropriate internet usage,
- CF 5.3.4.2 types and examples of prohibited site
- CF 5.3.4.3 the presence of monitoring , and
- CF 5.3.4.4 consequences for violating the Internet Policy.

The Internet Policy shall include methods to:

- CF 5.3.4.5 convey the content of the policy to users, and
- CF 5.3.4.6 ensure each user of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.3.5 Computer Software and IT Equipment

CF 5.3.5 The site shall establish, implement and maintain an Computer Equipment Policy (or a clause in an overarching Acceptable Use Policy) addressing the following:

- CF 5.3.5.1 the organization's software and IT equipment is exclusively for business use,
- CF 5.3.5.2 personal use and/or data storage is not permitted without express written authorization,
- CF 5.3.5.3 only software necessary for business functions shall be installed, and
- CF 5.3.5.4 audits to confirm only authorized, legal, and licensed software is installed.

Audits of installed software shall be conducted quarterly, with records, logs, and evidence of actions retained for six months.

- CF 5.3.5.5 convey the content of the policy to users, and
- CF 5.3.5.6 ensure each user of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.3.6 Secure Digital Asset Disposal Policy

CF 5.3.6 Establish a Secure Digital Asset Disposal Policy covering the following:

- CF 5.3.6.1 identification of what assets require secure and controlled disposal,
- CF 5.3.6.2 ensuring any personal or confidential information cannot be accessed by unauthorized persons,
- CF 5.3.6.3 labeling and tracking of assets requiring disposal,
- CF 5.3.6.4 where assets awaiting disposal are to be stored,
- CF 5.3.6.5 who can authorize disposal,
- CF 5.3.6.6 how local secure disposal occurs on and off site,
- CF 5.3.6.7 records of compliance to disposal process,
- CF 5.3.6.8 records of compliance to the disposal of potentially dangerous metals or recyclable components in accordance with applicable regulations,
- CF 5.3.6.9 safe procedures for the user,
- CF 5.3.6.10 safe procedures for the organization,
- CF 5.3.6.11 records of compliance from any subcontractors.

The Secure Digital Asset Disposal Policy shall include methods to:

- CF 5.3.6.12 convey the content of the policy to users, and
- CF 5.3.6.13 ensure each user of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.4 Infrastructure Security Measures

CF 5.4.1 Anti-Virus

CF 5.4.1 Establish an Anti-Virus Policy covering the following:

- CF 5.4.1.1 where Anti Virus software is to be deployed,
- CF 5.4.1.2 where Anti Virus software is to not be deployed,
- CF 5.4.1.3 why it is not deployed everywhere (if applicable),
- CF 5.4.1.4 what countermeasures will be implemented where Anti Virus software is not installed,
- CF 5.4.1.5 updates at least weekly on clients and at least daily on servers,
- CF 5.4.1.6 users shall not be able to disable the Anti Virus software,
- CF 5.4.1.7 Anti Virus shall perform on access scanning (on clients and servers),
- CF 5.4.1.8 Anti Virus shall undertake background scanning at least once per month on clients and weekly on servers,
- CF 5.4.1.9 Anti Virus shall be licensed and legally operated,
- CF 5.4.1.10 Anti Virus software shall at least quarantine the malware (deletion is an option).

The Anti-Virus Policy shall include methods to:

- CF 5.4.1.11 convey the content of the policy to users, and
- CF 5.4.1.12 ensure each user of the corporate infrastructure has been made aware, and agrees to comply with and be contractually and legally bound by its contents.

CF 5.4.2 Server and Workstation Usage Logging and Review

CF 5.4.2 Enable logging of the following:

- CF 5.4.2.1 any user, service, or system account creation,
- CF 5.4.2.2 deletion or suspension of any account,
- CF 5.4.2.3 change of any account's permissions,
- CF 5.4.2.4 successful logon attempts,
- CF 5.4.2.5 failed logon attempts,
- CF 5.4.2.6 where VPNs are used for remote workers, the logging shall include the username used to authenticate and the remote IP address from which they connected.

- CF 5.4.2.7 These logs are to be kept for at least 1 year and ideally removed onto CD/DVD/Blu-Ray media on a regular basis and stored in a secure location.
- CF 5.4.2.8 Record the implementation, management, and configuration control of the logging regime.
- CF 5.4.2.9 Establish a method for recording changes to the logging on the systems.

CF 5.4.3 Server and Workstation Patch Management

CF 5.4.3 The site shall have a documented server and workstation patching policy conforming to the following:

- CF 5.4.3.1 all servers shall be patched,
- CF 5.4.3.2 no server shall remain un-patched for more than 3 months,
- CF 5.4.3.3 no security barrier shall remain un-patched for more than 1 month,
- CF 5.4.3.4 where server patches are not implemented, the manufacturer's workarounds shall be implemented,
- CF 5.4.3.5 a record of server patches implemented and not implemented shall be maintained.
- CF 5.4.3.6 workstations shall be patched,
- CF 5.4.3.7 no workstation shall remain un-patched for more than 3 months,
- CF 5.4.3.8 where workstation patches are not implemented, the manufacturer's workarounds shall be implemented,
- CF 5.4.3.9 a record of workstation patches implemented and not implemented shall be maintained.
- CF 5.4.3.10 vulnerability analysis reports that include patch checking every 6 weeks,
- CF 5.4.3.11 consider pre-deployment patch testing to ensure patches will not break the operational system,
- CF 5.4.3.12 authority to patch systems,
- CF 5.4.3.13 establish Service Level Agreements (SLA's) to ensure that each business unit is fully aware of the requirement to patch at regular intervals and the likely timing and duration of such operations.

CF 5.4.4 Physical and Logical Information Asset Management

CF 5.4.4 Physical and Logical Information Asset Management

CF 5.4.4 The site shall maintain a register of its physical IT assets including the following characteristics:

- CF 5.4.4.1 classification of assets in both financial value and in terms of impact to the business,
- CF 5.4.4.2 identification of responsibility of staff with respect to level of protection of the assets to which they have access,
- CF 5.4.4.3 Board level visibility of high level risks of asset loss,
- CF 5.4.4.4 linked to the site's 'accounting' asset register,
- CF 5.4.4.5 restricted distribution and being read-only to those that need to check details,
- CF 5.4.4.6 ability to update the register shall only be held by a few authorized staff,
- CF 5.4.4.7 authorized staff shall have been background checked and deemed trustworthy,
- CF 5.4.4.8 asset serial numbers and descriptions,
- CF 5.4.4.9 normal asset location or in the case of mobile IT equipment, the designated holder,
- CF 5.4.4.10 a unique system identifier for the device which can be gathered using operating system auditing software and may include the MAC address of the LAN network card and the WLAN card and/or the operating system host name (Windows or Unix/Linux).

Personal or guest assets are not permitted to connect to the LAN or any part of the system. If it is deemed that visitors (contractors or clients) shall have access to IT services, then a separate guest LAN shall be implemented with the following restrictions:

- CF 5.4.4.11 the guest LAN can connect only to shared guest assets (e.g., file server, printers) cabled separately from the core corporate infrastructure,
- CF 5.4.4.12 guest assets shall be protected and monitored (e.g., behind a firewall controlled by passwords and having physical access protection),
- CF 5.4.4.13 separate connection to the internet can be provided for visitors working in the organization (e.g., contractors),
- CF 5.4.4.14 wireless access may be provided, but it shall be low-powered, appropriately secured and only in the areas necessary,
- CF 5.4.4.15 if the organization's assets connect to the guest LAN, they shall use a Virtual Private Network (VPN) to connect back to the organization.

To prevent data migration off the organization's systems, the use of remote email access and remote system access (except via an approved VPN link) shall be disabled. The following technologies are prohibited:

- CF 5.4.4.16 Log-Me-In,
- CF 5.4.4.17 Outlook Web Access (OWA),
- CF 5.4.4.18 PCAnyWhere,
- CF 5.4.4.19 externally accessible VNC,
- CF 5.4.4.20 non-encrypted Remote Desktop (RDP),
- CF 5.4.4.21 Windows Remote Assistance,
- CF 5.4.4.22 Internet Conference software (e.g., WebEx) may be permitted where a clear policy on its use is written and issued to staff with the business need to use the facility.

CF 5.4.5 Personal Device Usage

CF 5.4.5 Private or personal equipment shall not be connected to the site's hardware or LAN. As a minimum, the policy shall clearly prohibit the following items:

- CF 5.4.5.1 private MP3/MP4 players or iPods,
- CF 5.4.5.2 private mobile phones (including iPhones),
- CF 5.4.5.3 USB Sticks or other mobile/portable storage devices, and
- CF 5.4.5.4 any item of private equipment that is powered, charged, connected or used via a computer USB, parallel or serial port/connector.

Where a business requirement exists for guests to have internet access, this shall be established by the creation of a segregated Guest LAN. Preference would be for physically segregated network. Where this is impractical, logical network barriers shall be established.

CF 5.4.6 Wireless Security Usage and Protection

CF 5.4.6 The site must implement a wireless security policy including the following:

- CF 5.4.6.1 WPA2 is to be implemented between infrastructure and client connection,
- CF 5.4.6.2 where possible this shall be implemented via an infrastructure implementation, e.g., usingg AES and not TKIP encryption,
- CF 5.4.6.3 exceptions shall be isolated from the main network, which may include presentation screen control devices, presentation support devices that display data but do not cache or process it (e.g., media centers), and Window/blind control systems,
- CF 5.4.6.4 all methods to prevent un-authorized access shall be documented as a configuration control document, and
- CF 5.4.6.5 where controls are to be conveyed to employees, this shall be part of an acceptable usage policy.

CF 5.5 Personnel Training

CF 5.5.1 Basic Users Training

CF 5.5.1 All users shall undergo a minimum of 30 minutes of IT and digital security training every calendar year. The training shall cover:

- CF 5.5.1.1 good password selection,
- CF 5.5.1.2 use of personal data to create password is not recommended,
- CF 5.5.1.3 tips to remember passwords,
- CF 5.5.1.4 how to store passwords securely if it cannot be remembered,
- CF 5.5.1.5 how to identify a phishing attack,
- CF 5.5.1.6 how and when to report a phishing attack,
- CF 5.5.1.7 why users should not open unsolicited emails or attachments,
- CF 5.5.1.8 how to save a file to the desktop and run an AV scan of it,
- CF 5.5.1.9 how to check the Anti Virus software is up to date,
- CF 5.5.1.10 where to get free home use Anti Virus software for use at home,
- CF 5.5.1.11 how to lock/unlock their computer or system,
- CF 5.5.1.12 when to lock the computer (e.g., when unattended),
- CF 5.5.1.13 when to shut the computer down (e.g., at the end of the day),
- CF 5.5.1.14 how to secure their laptop assets,
- CF 5.5.1.15 how to report all security incidents relating to their operation of the workstation,
and
- CF 5.5.1.16 training records are required for shall detail student's name, training type,
training date, results of any exams, and validity of any exam,

CF 5.5.2 Advanced System Administrator Training

CF 5.5.2 The site shall have suitably trained system administrations, meeting the following requirements:

- CF 5.5.2.1 undertake a review of the systems used to determine the skills required for administrators to competently administer the system,
- CF 5.5.2.2 the administrators supporting the system shall have undertaken at least two of the following types of training course: Network Configuration, Platform Configuration, Introduction to Network Security, and Platform Specific Training or have demonstrated equivalent experience, and
- CF 5.5.2.3 maintain records of all administrator training.

CF 5.6 Additional Requirements for Digital Operations

CF 5.6.1 Regular Review of System Audit Logs

CF 5.6.1 The organization shall enable logging on all systems handling digital assets, develop a process to review the logs, and define a system to report findings and investigate anomalies.

Elements logged on all servers shall include the following:

- CF 5.6.1.1 any user, service or system account creation,
- CF 5.6.1.2 deletion or suspension of any account,
- CF 5.6.1.3 change of any account's permissions,
- CF 5.6.1.4 failed logon attempts, and
- CF 5.6.1.5 where VPNs are used for remote workers, the logging should include the username used to authenticate, and if possible, the remote IP address they connected from.
- CF 5.6.1.6 application logs,
- CF 5.6.1.7 backup logs, and
- CF 5.6.1.8 replication or synchronization logs.
- CF 5.6.1.9 all firewalls and boundary devices,
- CF 5.6.1.10 all servers,
- CF 5.6.1.11 all authentication points,
- CF 5.6.1.12 all applications that require any authentication,
- CF 5.6.1.13 all physical access to the servers or server rooms (not necessarily a digital log file),
- CF 5.6.1.14 where digital access control is implemented, access to a building that protects the servers or data stores,
- CF 5.6.1.15 the remote connection of any user to the LAN or RAS type node (both successful and failed attempts),
- CF 5.6.1.16 any attempt to change any security policy (both successful and failed attempts),
- CF 5.6.1.17 any reboot of any server, and
- CF 5.6.1.18 any restart of any service on any server.

Log settings must show that for Operating System authentication and applications that use or require authentication, the logging includes:

- CF 5.6.1.19 the event,
- CF 5.6.1.20 the importance of the event (e.g., "information", "error", "warning", or "critical"),
- CF 5.6.1.21 the time of the event, and
- CF 5.6.1.22 the server or node the event was recorded on.

Log files shall be kept for at least 1 year and ideally backed up onto CD/DVD/Blu-Ray media on a regular basis.

CF 5.6.2 Dedicated and Skilled Security Staff

CF 5.6.2 The organization shall define a dedicated IT security role separate from the network support team. Depending on the site of the organization this role may include multiple people on-site or off-site. The role may be performed by specialist third-party.

CF 5.6.2.1 Maintain records of security barriers employed and which parties are responsible to configure, maintain, and monitor these barriers.

CF 5.6.2.2 Undertake training and certification of personnel for the dedicated security barriers employed.

CF 5.6.3 Application Layer and Stateful Firewalls

CF 5.6.3 All connections from outside the organization shall be controlled by a correctly configured Application Layer Firewall. The firewall shall operate at Open Systems Interconnection (OSI) Layer 3 and shall be able to:

- CF 5.6.3.1 track both internal outbound requests and inbound external requests,
- CF 5.6.3.2 allow the returning responses to requests based upon information in its internal state table,
- CF 5.6.3.3 deny a connection to a timed out or dynamically closed connection,
- CF 5.6.3.4 block access from IP addresses to dynamically opened ports that are not available to that address (i.e., the state table entry does not match),
- CF 5.6.3.5 reject packets based upon its built-in Stateful Packet filtering, and
- CF 5.6.3.6 silently reject or drop packets from sources not approved for connection to or through the firewall.

The stateful firewall shall also operate to the following criteria:

- CF 5.6.3.7 OSI Layer 7,
- CF 5.6.3.8 configured to inspect the protocols passing through it and not set in a dumb proxy mode, and
- CF 5.6.3.9 configured to block protocols that are not required by the organization.

Additionally, the firewall shall:

- CF 5.6.3.10 inspect the DMZ traffic, where possible, and if the technology permits, break any SSL link to DMZ services and inspect that traffic,
- CF 5.6.3.11 be configured to only allow the minimum of services through,
- CF 5.6.3.12 include both inbound and outbound port filtering,
- CF 5.6.3.13 control outbound communication and not allow all outbound connections by default,
- CF 5.6.3.14 minimize the inbound connections,
- CF 5.6.3.15 be specific to defined IP addresses,
- CF 5.6.3.16 strictly limit connections into and out of DMZ servers and only to required ports,
- CF 5.6.3.17 provide a DMZ function for public facing servers (by itself or in conjunction with another Stateful Firewall),
- CF 5.6.3.18 be independently tested by a skilled person who confirms it is operating correctly and securely,
- CF 5.6.3.19 be managed from a dedicated system that is defined in the firewall rules to prevent others modifying the firewall,
- CF 5.6.3.20 be configured to alert the Administrator when (firewall hardware/software permitting):
 - rules have been changed on the firewall,
 - patches have been applied to the firewall,
 - the firewall has rebooted,
 - new updates are available for the firewall,
- CF 5.6.3.21 be included in the organization's patching policy and strategy.

Large organizations (more than 100 clients on the system) shall give strong consideration to implementing:

- CF 5.6.3.22 a standalone Web Proxy in the DMZ to reduce the impact of a web-based attack exploiting the clients or the internal proxy server, and
- CF 5.6.3.23 a standalone e-mail proxy in the DMZ to reduce the impact of an e-mail virus or other e-mail based attacks.

CF 5.6.4 Internal and Public-facing Server Hardening

CF 5.6.4 All public facing and internal servers shall be locked down (i.e., secured) and base-lined (i.e., its configuration defined, recorded and the system backed up fully and to read-only media).

For public facing servers, the documented hardening process shall include, cover or ensure:

- CF 5.6.4.1 The servers shall be patched to the highest level possible.
- CF 5.6.4.2 The servers are backed up in the secure configuration.
- CF 5.6.4.3 Removing all unnecessary services or ensuring that they are disabled.
- CF 5.6.4.4 Servers do not have any internal network credentials entered, stored or cached.
- CF 5.6.4.5 A server has never been added to the internal domain.
- CF 5.6.4.6 A server administrator/root account and password used in the installation are not used on the internal domain/administrator account.
- CF 5.6.4.7 Servers shall never be, or have been, members of the internal domain.
- CF 5.6.4.8 Servers shall never be, or have been, used as general systems.
- CF 5.6.4.9 Servers shall never be, or have been, used to browse the internet.
- CF 5.6.4.10 Servers shall never be, or have been, used to read publicly received email.
- CF 5.6.4.11 Any new server that is to be public facing shall be built in to a secure specification as dictated by recognized good practice documents.
- CF 5.6.4.12 The server shall be built from a known good data source.
- CF 5.6.4.13 The server shall be patched before being connected to the internet.
- CF 5.6.4.14 The server shall be hardened before being exposed to the internet, not installed in the Demilitarized Zone (DMZ) and built in place.
- CF 5.6.4.15 Server administrator accounts shall not use the same names or passwords as for internal LAN servers.
- CF 5.6.4.16 All servers reusing Hard Disk Drives (HDD) shall be wiped, where every sector of the HDD is overwritten rather than formatted, to ensure no remnants of other user credentials exist.

For internal servers, the documented hardening process shall include, cover or ensure:

- CF 5.6.4.17 All unnecessary services and software items are disabled or removed.
- CF 5.6.4.18 The servers shall be patched to the highest level possible.
- CF 5.6.4.19 The servers shall be backed up in the secure configuration, so a baseline is held, shall the system need to be reverted to its initial configuration.
- CF 5.6.4.20 The servers shall not be used as general purpose systems.
- CF 5.6.4.21 The servers shall not be used to browse the internet.
- CF 5.6.4.22 Internal servers shall never have been part of the Organization's DMZ (as they could be importing Trojans, root kits or other software to assist an attacker).

Penetration testing by a qualified third party is strongly recommended on a regular basis.

CF 5.6.5 Remote Access Control

CF 5.6.5 The organization shall develop and policy and system to ensure only the organization's assets shall be permitted to connect to the network. The policy and system shall address:

- CF 5.6.5.1 a method to approve access to the corporate environment,
- CF 5.6.5.2 limits access to approved devices (e.g., machine passwords vs. VPN passwords and non-exportable certificates on mobile assets), and
- CF 5.6.5.3 records and monitors remote access.

CF 5.6.6 Virtual Private Networks and Encryption

CF 5.6.6 The organization shall document any remote VPN connections and record:

- CF 5.6.6.1 the reason for each connection,
- CF 5.6.6.2 the users of each connection, and
- CF 5.6.6.3 how the use is to be controlled and monitored.

Where long-standing relationships exist, encryption has be implemented on communication links along the following principles:

- CF 5.6.6.4 e-mails shall be digitally signed by staff,
- CF 5.6.6.5 mobile devices shall use VPN links and not communicate in the clear (regardless of ISP/Telecom provider claims about private clouds),
- CF 5.6.6.6 core business point-to-point connections shall be via VPN or be SSL encrypted,
- CF 5.6.6.7 VPN or encryption should be considered at the router level,
- CF 5.6.6.8 VPN or encryption shall be considered for firewall-to-firewall links, and
- CF 5.6.6.9 Public Certificate Authorities (CAs) do not need to be used; internal CAs can be adopted.

CF 5.6.7 Mobile Device Lockdown and Encryption

- CF 5.6.7 The following shall be implemented for locking down and encrypting mobile devices:
- CF 5.6.7.1 BlackBerry and other mobile devices shall be encrypted where solutions are available,
 - CF 5.6.7.2 a locking code (PIN) shall be implemented that prevents access to the stored data or functions (not including phone answering capabilities),
 - CF 5.6.7.3 in the event that the user fails to enter the correct PIN/code 5 times consecutively it shall result in a lockout which requires a manufacturer to reset. The device shall wipe its internal volatile memory, and
 - CF 5.6.7.4 the organization initiates a remote wipe upon receiving information that the device is lost or compromised.

CF 5.6.8 Peripheral Device Management, Control, and Audit

- CF 5.6.8 The organization shall define a policy and method to manage, control, and audit peripheral devices including the following:
- CF 5.6.8.1 a policy governing the use of USB devices (and similar),
 - CF 5.6.8.2 the right to examine all USB devices (and similar) upon entry to or exit from the site,
 - CF 5.6.8.3 the right to deny an employee, visitor, contractor, or third-party to bring a USB device (and similar) on to the site,
 - CF 5.6.8.4 auditable method to trace use of USB devices (and similar) including the data moved to/from the device, and
 - CF 5.6.8.5 infringement of the policy shall result in confiscation of the device as an absolute right of the organization to prevent data loss.

CF 5.6.9 Implemented, Managed, and Enforced Configuration Control

- CF 5.6.9 The organization shall develop a process and procedures to control software according to the following:
- CF 5.6.9.1 define a role to approve changes to the system,
 - CF 5.6.9.2 define a process to select new software,
 - CF 5.6.9.3 prevents users from installing and uninstalling software,
 - CF 5.6.9.4 prevents users from disabling any security product, and
 - CF 5.6.9.5 maintains a system-by-system inventory of approved software.

CF 5.6.10 Advanced Security Personnel Training

- CF 5.6.10 The organization shall ensure IT security personnel are qualified for their role, which includes:
- CF 5.6.10.1 a review of the systems being employed to document security related skill sets are required to protect systems from unauthorized attack or compromise,
 - CF 5.6.10.2 a summary of skills attributed to IT security personnel, and
 - CF 5.6.10.3 maintain records of continuing training and certifications of IT security personnel.

CF 6 TRAINING AND AWARENESS

CF 6.1 Defined Training and Awareness Needs

Training and awareness approaches shall ensure that the requisite knowledge, skills, capabilities, internal controls and security awareness levels are maintained to meet security management system specifications and security plans.

CF 6.2 Provision of Training

Management shall identify training needs, budget resources, and conduct training in security policy and content security management system processes and/or procedures. Personnel shall have the capability to fulfill their respective roles and responsibilities on the basis of education, training and awareness. Records of such training shall be maintained for at least 3 years.

CF 6.3 Personnel Understanding of Security Management System

Personnel shall understand the security policy, and content security management system processes and procedures through new hire orientation, on-going training and other appropriate means, and have piracy awareness, as appropriate.

CF 6.4 Training Records

CF 6.5 Provision of On-going Security Management System Awareness

Management shall promote and ensure effective communication and awareness of the content security management system processes and policies within and between relevant areas of the organization in a manner that encourages involvement of personnel in achieving content security and continual improvement. Additions and changes in the security policies, security process, procedures and related technologies shall be communicated, where appropriate. Consideration shall also be given to communication to vendors and third parties to ensure that content security is maintained.

CF 6.6 Avenues for Personnel Participation in Security Management System

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 7 DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

CF 7.1 Recovery and Continuity Plans

- CF 7.1.1 Management shall establish, implement and maintain methods to deal with disasters, unexpected events, and emergencies and help ensure that the confidentiality, integrity and availability of assets are maintained.
- CF 7.1.2 Management shall maintain disaster recovery and business continuity plans, including methods for continuity planning, initiating and executing contingency operations, recovery operations and resumption of normal operations, proper backup processes, testing, and process and asset restoration, where applicable. The site shall develop plans, which align with site business, contractual and/or Service Level Agreement (SLA) requirements.
- CF 7.1.3 This plan shall:
- CF 7.1.3.1 • include both systems and people,
 - CF 7.1.3.2 • identify the critical people and assets in the organization,
 - CF 7.1.3.3 • identify the critical aspects of the business,
 - CF 7.1.3.4 • detail high level and some detailed steps to take following an incident,
 - CF 7.1.3.5 • be supported by management (e.g., written endorsement), and
 - CF 7.1.3.6 • cover physical, technical and human based incidents.
- CF 7.1.4 Business continuity plans shall be tested through a simulated exercise.

CF 7.2 DRP/BCP

CF 7.2.1 The DRP/BCP shall define methods to:

- CF 7.2.1.1 detect and respond to external and environmental threats and their impacts from fire, smoke, temperature, water/flood, earthquake, lightning, vandalism, and other environmental threats and disasters, and ensure employees and others working on its behalf protect themselves and assets in the event of an emergency,
- CF 7.2.1.2 communicate during disasters,
- CF 7.2.1.3 prevent of power interruptions,
- CF 7.2.1.4 back-up, store, restore and protect of content and other assets to ensure their confidentiality, integrity and availability,
- CF 7.2.1.5 review and test plans for effectiveness, and to record test results, and
- CF 7.2.1.6 record preventive and corrective actions to maintain the integrity of assets and systems.