Music Recording Studio Security Program

Security Assessment

Version 1.1

DOCUMENTATION, RISK MANAGEMENT AND COMPLIANCE
PERSONNEL AND RESOURCES
ASSET MANAGEMENT
PHYSICAL SECURITY
IT SECURITY
TRAINING AND AWARENESS
INCIDENT MANAGEMENT AND RECOVERY PLANNING

ABOUT THIS PROGRAM

This program has been jointly developed by operational and technical specialists within the recording industry. The objective of the Music Recording Studio Security Program (MRSSP) Assessment is to establish a set of effective security controls that can measure how a Recording Studio or individual involved in the recording studio process will secure and protect physical and digital media assets. In order to mitigate the risk and reduce the impact of copyright infringement as a result of leaked content, focus has been placed on the access to and handling of physical and logical media assets.

The objective-based approach will only test applicable elements taken from the seven frameworks of capability used in the full version of the CDSA Security (CPS) Standard. The areas to be considered are:

RECORDING STUDIO SECURITY PROGRAM

- **CF 1: DOCUMENTATION, RISK MANAGEMENT AND COMPLIANCE**
- **CF 2: PERSONNEL AND RESOURCES**
- **CF 3: ASSET MANAGEMENT**
- **CF 4: PHYSICAL SECURITY**
- **CF 5: IT SECURITY**
- **CF 6: TRAINING AND AWARENESS**
- **CF 7: INCIDENT MANAGEMENT AND RECOVERY PLANNING**

According to the nature of operations a successful assessment against the relevant requirements will result in a site and/or an individual achieving approved site or service provider status.

The programs objectives are to identify, assess, manage and minimize risks to an acceptable level, thereby ensuring the continued integrity of intellectual property, confidentiality and media asset security.

The identified objectives provide the basis on which to define the auditable requirements for approved Site and/or service provider status.

The Assessment Process

On receipt of an application to join the program a CDSA auditor will be assigned and will contact the applicant to set a timeframe for the assessment and assist with preparation.

A one-day visit to the site or applicants place of work will take place followed by the submission of a detailed report.

A further assessment can be undertaken every 12 months thereafter in order to maintain approved site or service provider status.

A qualified CDSA auditor with relevant industry experience will carry out the audit.

The applicant receives approved status if:

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

An applicant will fail to achieve approved status where one or more major or systemic non-compliances are observed. Approved status can be awarded once major non-compliances have been adequately addressed, re-evaluated and accepted by CDSA.

How to use this document

In order to remain applicable to a wide cross-section of participants this document remains vendor and technology neutral. The Standard utilizes the following terms:

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

A the applicant may be referred to as 'site' or Service Provider. A site or service provider may form part of a larger organization.

The Statement of Applicability

The inaugural audit process will incorporate completion of a "Statement of Applicability" or SoA assisted by the assigned CDSA auditor. This document will define the scope of the assessment.

- Requirements deemed **Not Applicable** will be identified, justified and agreed.
- Requirements deemed **Applicable But Not Implemented** may be identified and accepted as:
    - In progress
    - Future project
    - Accepted risk
- Requirements **Not Addressed** may be accepted using equivalent compensating controls that meet the same objective.

Within each capability framework a summary of requirements has been provided to assist the applicant with their preparation. Further guidance is available through consultation with the appointed auditor or territory director.

Summary: Descriptive text to assist the applicant with the requirements to be met.

Objective: A measureable objective to be achieved.

Evidence: Items that may be accepted as demonstrating compliance.

Declination of Liability

CDSA has made every effort to formulate a program that they believe will help companies reduce the likelihood of content loss or theft. However, a program, no matter its specificity or diligent application, cannot guarantee avoidance of a claim. Therefore, CDSA must decline any liability toward the company or third party on account of this program, whether or not CDSA has issued a certificate.

CF 1.	DOCUMENTATION, RISK MANAGEMENT AND COMPLIANCE
CF 1.1.	**Documentation**
Summary:	CF 1.1 **Produce** and maintain relevant security policies, procedures and practices. Supported and authorized, where applicable, by management. Such documents set the context and provide the structure for communicating security expectations.
Objectives:	Develop and produce adequate security policy, procedures and associated documentation. Where relevant communicate all security policies, procedures and work instructions to staff. Ensure documents remain current and fit for purpose through a process of review.
Evidence:	Security Policy and Procedures Security Manual Associated documentation such as session reports.

CF 1.2.	Risk Management
Summary:	CF 1.2 **D**emonstrate how operational risk has been identified, assessed, treated and/or mitigated to an acceptable level. Documentation shall be assessed according to the level of complexity.
Objectives:	Conduct regular review of all business activity directly or indirectly associated to media assets in physical or digital format. Demonstrate that potential security related risks have been identified. Demonstrate that proportionate and effective controls have been implemented to treat and/or mitigate identified risks. Manage and review risks within a process of continual review.
Evidence:	Risk assessment methodology Documented risk assessments Completed Statement of Applicability Management review documents

CF 1.3.	Compliance
Summary:	CF 1.3 Methodology for ongoing compliance with the program shall be demonstrated. This should include effective incident management and a process of continual monitoring and review.
Objectives:	To ensure ongoing program requirements and any, legal, regulatory and contractual obligations have been considered. To provide a mechanism to promote on-going compliance.
Evidence:	Incident handling policy, procedures and completed Incident reports Corrective and preventive actions CDSA CPS audit report including associated non-compliances Management reviews

CF 2.	PERSONNEL AND RESOURCES
CF 2.1.	**Personnel and Resources**
Summary:	CF 2.1 The creative process can often, involve sharing of content between multiple resources working on the same project. When working in a shared environment, it is crucial to ensure that all parties involved with the project understand and adhere to program and requirements. A manager shall be nominated as being accountable for security functions. Individuals shall undertake responsibilities for ensuring the security requirements of this program are met. The level of background screening to be carried out on all personnel and resources, including contractors, consultants and third-party vendors shall be demonstrated. The program member must be capable of providing personnel and resources to meet the requirements of any, legal, regulatory and contractual obligations.
Objectives:	Mitigate the risk to content where personnel and resources are involved, including the engagement of contractors, consultants and third-party vendors.
Evidence:	Organizational structure depicting responsibility for security and program management Policy and procedural documentation Evidence non-financial processes that assist security and Service Level Agreements, third-party contracts, confidentiality and non-disclosure agreements Processes for the engagement of third-parties

CF 3.	ASSET MANAGEMENT
CF 3.1.	**Administrative Controls**
Summary:	CF 3.1 **s**ets out accountability, roles and responsibilities for asset management. Specific consideration should to be given to the types of asset being handled. The level of security afforded to assets must be consistent with risk assessment. An asset may be defined as: • Intellectual property, all formats of content including edits, rough cuts, un-mastered and mastered content and including any proprietary or sensitive information relating to a project. The asset may be in a physical, digital or electronic form and may exist at any point in the creative process. Each project should be assessed on an individual basis for risk and value, with any special requirements for high security projects being added to documentation. Administrative control of computer systems and storage locations containing digital IP or other commercial assets must be considered in line with the requirements as set out in section CF 5 of this program.
Objectives:	Ensure that accountability, roles and responsibilities for asset management and security are established and have been clearly communicated. Ensure a consistent approach when handling assets using a process of risk assessment. Provide a secure, efficient and effective operating system for all assets. Ensure additional security requirements are considered and implemented where necessary. Provide a chain of custody for assets.
Evidence:	Defined asset management roles and responsibilities Documented risk assessment Asset handling procedures Session reports Work orders and associated documentation

CF 3.2.	Asset Controls
Summary:	CF 3.2 All processes undertaken must be auditable. All original material and subsequent assets created, as part of a project, process or procedure must be included.
Objectives:	Implement, operate and maintain an accurate asset management system that is capable of audit.
Evidence:	Asset management system Asset management records Session reports Work orders and associated documentation

CF 3.3.	Asset Receipt and Identification
Summary:	CF 3.3 sets out the requirement to establish a mechanism for recording the receipt and identification of assets.
Objectives:	Implement, operate and maintain accurate records for asset receipt and future identification.
Evidence:	Physical and Electronic methods used for asset identification

CF 3.4.	Asset Handling and Transfer
Summary:	CF 3.4 The program member will be required to demonstrate work flows as well as the appropriate use of protective controls such as watermarking, password protection, encryption, use of secure and/or vendor approved digital delivery platforms, secure file transfer and secure or offline storage.
Objectives:	**O**perate and maintain effective processes for secure asset handling and transfer. Maintain accurate and accountable records of all asset movement that are capable of audit.
Evidence:	Asset tracking processes, policy, procedures and processes Asset handling policy, procedures and processes Third-party contracts, service level agreements (SLA's) and confidentiality agreements Asset tracking logs and/or manual records Use and application of asset protection technologies

CF 3.5.	Secure Asset Storage and Reconciliation Controls
Summary:	CF 3.5 sets out how the program member must ensure that assets are retained securely within secure areas.
Objectives:	Maintain accurate records for asset storage and movement. Ensure asset integrity and security is being maintained.
Evidence:	Inventory records and asset registers Cyclic count policy and procedure Documented reviews of cyclic count records Documented resolution and review of discrepancies Client notification policy and process Third-party contracts, service level agreements (SLAs) and confidentiality agreements Asset tracking logs and/or manual records

CF 3.6.	Asset Re-call Procedures
Summary:	CF 3.6 sets out requirements for monitoring assets allocated to an individual. Dependent on the activity and type of asset, different procedures may exist. However, the program member must demonstrate that it has taken into consideration the risk to high security items.
Objectives:	Prevent assets from being retained outside secure storage locations any longer than is necessary. Reduce opportunity for theft and prevent assets from being left unattended. Provide a mechanism whereby escalation procedures can be implemented, including commencement of checks, controls, investigation and client notification.
Evidence:	Asset management systems Inventory records Asset recall policy or process Incident management and investigation Policy and procedures for loss of asset and client notification Service level agreement or contractual requirements.

CF 3.7.	Control of Blank Media Materials
Summary:	CF 3.7 Unless properly controlled, access to blank media materials provides an opportunity to transfer, copy or transmit media files without detection. Policy, procedure or a process as appropriate must control the use of blank media materials. Blank media may include CDR, tapes, data storage etc..
Objectives:	Treat the use of blank media as an asset. Document, implement and maintain secure policy and processes for controlling raw material. Use of media duplication policy and guidelines
Evidence:	Policy, procedures and management records for asset identification, issue, tracking, return and destruction Cyclic count reconciliation policy, procedures and inspection results Media duplication guidelines

CF 3.8.	Record Retention
Summary:	CF 3.8 sets out the requirements for the retention of asset management records.
Objectives:	Retain accurate and detailed asset management records to enable and assist audit and investigation.
Evidence:	Asset retention policy and procedure Retained asset management records

CF 3.9.	Transportation of Assets
Summary:	CF 3.9 The secure transportation of assets off-site varies according to the type of activity, asset, technology, destination and contractual obligation.
Objectives:	Achieve secure transfer of assets between sites.
Evidence:	Policy and procedures for asset transportation Shipping records Third-party service level agreements and insurance

CF 3.10.	Destruction and Recycling
Summary:	CF 3.10 sets out requirements for the destruction and recycling of assets. During the creative process physical assets are often created that require secure and responsible destruction.
Objectives:	Secure and segregate assets while awaiting destruction. Securely destroy and recycle assets using a reliable and auditable process.
Evidence:	Asset destruction and recycling policy and procedures Destruction records and certificates of destruction Third-party Service Level Agreements Destruction and storage facilities

CF 4.	PHYSICAL SECURITY
CF 4.1.	**Physical Security Management**
Summary:	CF 4.1 The program member will be required to demonstrate the different levels and/or types of physical security controls used. This will be proportionate to the operational environment and activity undertaken. Policy, procedures and processes will help to demonstrate how proportionate and effective controls are maintained. Physical security may be applicable to a site location, internal location or device.
Objectives:	Implement security controls to safeguard media and operational assets. Demonstrate how unauthorized physical access to perimeter and internal secure areas is prevented, monitored and managed. Demonstrate how physical access is authorized, monitored and managed. Demonstrate how physical access controls protect media and operational assets and critical business information.
Evidence:	Physical security plans Physical security policies and procedures Physical security risk assessment methodology Physical security controls and boundaries Use of perimeter security, CCTV, Access Control, Keys, intruder detection, searches and physical device security Policy and procedures for internal controlled and secure locations

CF 4.2.	Securing Internal Areas
Summary:	CF 4.2 sets out the requirements for defining, segregating and working within controlled and secure internal areas. 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 bespoke physical security requirements.
Objectives:	Ensure the internal security of a site, and identify requirements for high security zones. Monitor, secure and control access to internal areas where media assets are located, stored, handled or produced.
Evidence:	Policy and procedures for internal controlled and secure locations Physical security controls and boundaries Event logs for access controls CCTV records Incident reports Visitor logs Search records Policy and procedures for visitors

CF 4.3.	Use of Guards
Summary:	CF 4.3 The use of guards is dependent on the nature of operations and risk assessment. A decision to instruct guards is decided by the evel of risk, access to resources and the availability of alternative controls, security systems or technology.
Objectives:	Ensure the integrity and security of the physical site by the use of guards.
Evidence:	Assignment instructions and any associated records Service level agreement with providers

CF 4.4.	Searches
Summary:	CF 4.4 A decision to search should be based on risk assessment. Consideration should be given as to who is being given access, the activity undertaken and the sensitivity of the content. Examples may include but not exclusively be playbacks and listening sessions.
Objectives:	Deter and detect the theft or misappropriation of assets.
Evidence:	Search policy and procedures Search records

CF 4.5.	CCTV
Summary:	CF 4.5 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. As a guide images must be: • 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 to aid investigation, • Processed in accordance with an individual's human rights, and • Kept secure and only accessible by those who have a business need.
Objectives:	Protect premises, staff and media assets through the effective use of CCTV.
Evidence:	Policy or integration of policies for CCTV Management controls for CCTV imagery Maintenance records SLA and confidentiality agreements

CF 4.6.	Access Control Systems and Automated Technologies (AACS)
Summary:	CF 4.6 sets out the security requirements for the use access control systems including automated technologies (AACS). 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.
Objectives:	Protect external and internal access to controlled and designated internal secure areas through the use of access control.
Evidence:	Access control policy and procedures Access control plan Access control logs Maintenance records SLA and confidentiality agreements

CF 4.7.	Intruder Detection Systems (IDS)
Summary:	CF 4.7 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.
Objectives:	Detect the entry, or attempted entry of an intruder into a protected area. Identify the location of the intrusion and to signal an alarm on which to respond.
Evidence:	IDS policy and procedures Alarm response records Event logs Maintenance reports Uninterrupted powers supply (UPS) SLA and confidentiality agreements

CF 5.	IT SECURITY
CF 5.1.	**Information Security Policy**
Summary:	CF 5.1 Documents shall demonstrate the technical security controls and practices in place. IT infrastructure consists of the equipment, systems, software, and services including all hardware, networks and facilities.
Objectives:	Establish a basic document framework for IT controls.
Evidence:	IT security policy framework IT security plans

CF 5.2.	Acceptable Use
Summary:	CF 5.2 Acceptable use is a rule set defined by the program member that restricts the way in which IT systems, networks and assets may be used including internet, social media and email.
Objectives:	Provide a formal framework for acceptable system, network, asset and internet usage. Achieve a culture of responsible behavior at all levels of the organization when working with client assets. Achieve a culture of responsible Internet usage
Evidence:	Acceptable use of IT systems policy Individual's acceptance of policy Management review

CF 5.3.	System Administrator and Elevated Privilege User Accounts
Summary:	CF 5.3 sets out the requirements for administrator and elevated privilege user accounts. These elevated privileges may allow the creation, modification and access to local user groups, folders and accounts, to delete files, install hardware/software, modify the operating system and configure network/firewall settings. Such activities must be controlled with clear segregation of duties established within policy. See CF 6 for training and awareness requirements.
Objectives:	Define, control and securely manage persons with administrator/elevated privilege level access to network/systems and logical media assets
Evidence:	Administrator and elevated privilege user policy and procedures Administrator and elevated privilege account logs Change management requests Firewall logs Training and awareness records Individual's acceptance of policy

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.
Objectives:	Define, control and securely manage persons with basic user level access to network/systems and logical media assets.
Evidence:	Administrator and elevated privilege user policy and procedures Administrator and elevated privilege account logs Change management requests Firewall logs Training and awareness records Individual's acceptance of policy

CF 5.5.	Password Management
Summary:	CF 5.5 sets out requirements for password management. Passwords are the front line of protection for user accounts and network access. Rules must be in place to separate and define the complexity, length, use and re-use for system level and user passwords.
Objectives:	Ensure the program member has appropriate and consistent password controls to deter unauthorized access to IT systems.
Evidence:	Password policy Administrator controls and monitoring Individual's acceptance of policy

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. Access to company information via IT systems must be controlled, risk assessed, authorized and documented.
Objectives:	To maintain integrity and security of IT systems/networks and logical media assets accessed by third-parties.
Evidence:	Third-party access policy and procedures Records of authority Log files Policy acceptance SLA, NDA and confidentiality agreements

CF 5.7.	Removable Media
Summary:	CF 5.7 sets out requirements for controlling removable media and personal devices. Removable media represents a significant threat to the loss or compromise of media assets. Such media may be owned/controlled by the site or an individual.
Objectives:	To ensure controls are in place to prevent unauthorized removal from the site and or any device or introduction of threats to IT systems.
Evidence:	Policy to manage removable media Authorization records Network access controls Asset register Device identification

CF 5.8.	Mobile Device Management
Summary:	CF 5.8 sets out the requirements for acceptable use of mobile and portable devices capable of processing, transmitting or storing sensitive company data or client information.
Objectives:	Set a formal requirement for mobile device acceptable use. Achieve a culture of responsible behavior when working with mobile devices.
Evidence:	Mobile device acceptable use policy Device register Authorization records Users' acceptance of policy

CF 5.9.	Wireless Networks
Summary:	CF 5.9 sets out the requirements for wireless networks. Sites and/or devices using wireless networks need to carefully consider the deployment of wireless networks within a production or manufacturing environment.
Objectives:	Secure wireless networks to prevent unauthorized access or loss of sensitive data.
Evidence:	Wireless network policy Network maps Authentication strategy Encryption strategy

CF 5.10.	Physical and Environmental Security Controls
Summary:	CF 5.10 sets out the requirements for physical and environmental security controls. Data and logical media assets must be physically as well as logically protected.
Objectives:	Ensure data and logical media assets are physically controlled and secured. Ensure environmental conditions are managed.
Evidence:	Server room and data store policy and procedures Physical controls to monitor and control access Environmental protection systems Inspection reports Routine maintenance reports Third-party SLA and confidentiality agreements

CF 5.11.	IT Asset Management
Summary:	CF 5.11 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, is to be maintained. Physical assets should be marked, referenced or have bar code registration. Software assets and applications should be registered. The destruction or removal from use of all hardware and associated digital assets must be properly authorized.
Objectives:	Provide a register of all hardware, associated devices and software in use. Ensure that regular reviews of software use are undertaken. Ensure data from defective hardware is securely removed prior to any authorized repair. Ensure that redundant hardware and associated devices are disposed of properly in a secure manner that prevents data migration.
Evidence:	Policy to register, use and destroy hardware and associated devices Authorization records Network access controls Asset register Device identification Software management solutions Data removal policy Repair service level agreements (SLAs) Destruction certificates

CF 5.12.	Network Monitoring
Summary:	CF 5.12 sets out the requirements for monitoring network activity. Where relevant systems must be monitored to detect unauthorized processing activities. Information security events are to be logged, reviewed, recorded and investigated where required.
Objectives:	Ensure networks are monitored effectively.
Evidence:	Demonstrate how network traffic is monitored Event logs Demonstrate actions to be taken in the event of anomalies Records of any e-mail/SMS alerts

CF 5.13.	Access Controls
Summary:	CF 5.13 sets out the requirements for authorizing and controlling access to network systems. Access controls can be both physical and logical (i.e., tools used to identify, authenticate or authorize users on computer systems).
Objectives:	Effectively manage access controls.
Evidence:	Policy and process to identify and control access Access control lists (ACLs) and logs Complete configuration management reviews

CF 5.14.	Remote Access
Summary:	CF 5.14 sets out the requirements for authorizing and accessing network systems from remote locations. Remote access controls must be enforced to mitigate the risk of loss or compromise to client content.
Objectives:	Establish effective controls to secure remote access requirements.
Evidence:	Policy and process to identify and control access. Evidence of ACL's logs. Present records of configuration reviews

CF 5.15.	Change Management
Summary:	CF 5.15 sets out the requirements for ensuring that all system configuration changes are properly authorized, tested and implemented. Change management will depend on the size and nature of operations.
Objectives:	Effectively manage change within the site's networks.
Evidence:	Policy and process to manage change Evidence of effective change Document configuration reviews

CF 5.16.	System Documentation
Summary:	CF 5.16 sets out the requirements necessary to demonstrate the full network landscape. A clear and well-defined system architectural document allows immediate and easy reference to the network landscape. Document detail and complexity will depend upon the size and nature of operations.
Objectives:	Effectively document the systems architecture of all networks.
Evidence:	System architecture policy or reference to production of system architecture Method of safeguarding presentational information Network landscape diagram

CF 5.17.	External Networks
Summary:	CF 5.17 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).
Objectives:	Maintain the security of external networks.
Evidence:	Intrusion detection logs

CF 5.18.	Internal Networks
Summary:	CF 5.18 sets out the requirements necessary to ensure proper separation of network functions. For example Internal networks with no direct internet access. There may be multiple internal segments according to functions.
Objectives:	Maintain the security of internal networks. Ensure separation of administrative functions
Evidence:	Network maps (architectural diagrams) Intrusion detections system logs Separation of administrative functions

CF 5.19.	File Transfer Management
Summary:	CF 5.19 sets out the requirements relating to file transfer technologies and encryption of data. File transfer technologies in this context are those information exchange systems approved and used by content owners to distribute media to their supply chains and end users. The site must have full knowledge and oversight of all such technologies in use.
Objectives:	Ensure effective file transfer methodologies and encryption.
Evidence:	Policy for the use of all file transfer and encryption technologies Log files to prove controls are clearly understood and practiced

CF 5.20.	Firewall Management
Summary:	CF 5.20 sets out the requirements for firewall management. Firewalls control traffic flow between a trusted network and an untrusted or public network (e.g., internet). It is essential that program member protect IT systems from untrusted networks by way of an approved firewall. The program requires that firewalls must be correctly configured to reduce risk and deal appropriately with any threats that may be encountered. A formal system of review and logging is necessary to ensure an adequate level of protection.
Objectives:	Ensure effective firewall management.
Evidence:	Record of the use and configuration of devices deployed Evidence that devices are configured, controlled and reviewed regularly

CF 5.21.	Vulnerability Management
Summary:	CF 5.21 sets out the requirements necessary for vulnerability management. Applying a regime of good housekeeping can mitigate the majority of vulnerabilities. If not protected and updated, systems can become unstable, causing loss of data, which if not backed up can cause permanent loss or compromise of client assets. Vulnerability management seeks to eradicate these threats through proper application of: • Anti-virus, • Security updates, • Server and system build configuration back-ups, • Regular data back-ups, • Vulnerability scanning, • Testing.
Objectives:	Ensure effective anti-virus is installed and maintained. Ensure that regular security updating reduces vulnerabilities. Ensure that server and system configuration back-ups are available in the event of an unplanned incident. Ensure that data maintains integrity and confidentiality in the event of a loss of services.
Evidence:	Documented configuration of devices deployed Evidence that devices are configured, controlled and reviewed regularly

CF 6.	TRAINING AND AWARENESS
CF 6.1.	**Training and Awareness Needs**
Summary:	CF 6.1 sets out the requirements for security awareness. All employees, contractors, consultants and third-parties must be capable of delivering their services securely and shall be made aware of the security measures and requirements used to protect the confidentiality and integrity of customer assets and intellectual property.
Objectives:	Ensure all personnel are competent and made aware of security requirements.
Evidence:	Security training policy Training records

CF 7.	INCIDENT MANAGEMENT AND RECOVERY PLANNING
CF 7.1.	**Incident Management and Recovery Planning**
Summary:	CF7.1 Incident Management and Recovery planning sets out the requirements for Incident management and recovery planning. A process and ability to ensure investigation and recovery in the event an incident shall be demonstrated. The degree of complexity and ability to recover will be dependent and commensurate to the size and nature of operations. Events to be considered may include but are not exclusive to natural disaster, fire, flood, accident, civil unrest, equipment failures and deliberate or malicious acts of sabotage.
Objectives:	To ensure the confidentiality, integrity and availability of client assets are maintained in the event of an unexpected or significant event or emergency. To minimize the impact on clients in the event of an unexpected or significant event or emergency.
Evidence:	Business continuity plan and disaster recovery plan Management reviews and test results