Content Security

RECOMMENDED BEST PRACTICES

for PRODUCTION & POST PRODUCTION / EDITORIAL

Version 16.2

MANAGEMENT CONTROLS

PERSONNEL AND RESOURCES / PRODUCTION OFFICE

ASSET MANAGEMENT / CAMERA MEDIA

PHYSICAL SECURITY

IT SECURITY

TRAINING AND AWARENESS

INCIDENT MANAGEMENT AND RECOVERY PLANNING

EDITORIAL / DIGITAL WORKFLOW

SCRIPT HANDLING

INTRODUCTION

The aim of this framework is to recommend Best Practices for securing content and confidential information on-location productions and the post-production editorial spaces.

It is very important that the assessment of risks in these areas to be completely without interruption to the creative process, and should not interfere with the operational efficiencies of the Production and Post Production / Editorial process.

The process is designed to encompass all stakeholders in the Production and Post Production / Editorial process. The objective is to promote a responsible security culture on commencement of the project and to introduce a structured approach when determining security requirements

During the projects planning phases an initial assessment against the Recommended Best Practices will be completed to identify any potential risks that need consideration. Component elements for content protection and the types of assets to be protected will be identified. Personnel to be engaged should be properly briefed in advance of the risk assessment.

An assessment report will be submitted to the project management team. The report will consider the relevant controls suggested for consideration to increase security and mitigate risk of loss of content or confidential information during the project and make recommendation on implementation. The assessor will remain available to assist development as instructed.

The result of the initial assessment will be documented on an Assessor Checklist (Appendix 'A'). Not all projects will require every Operational Recommendation, therefore where not applicable the reason will be recorded within the Assessor Checklist.

The security Recommended Best Practices utilize 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.

Recommendation: 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

1 MANAGEMENT CONTROLS

1.1 Documentation

· Produce and maintain a set of security documents or work instructions for content and site security.
· Disseminate security related requirements to all persons engaged on the project. Include any remote locations and third parties. Set out specific roles and responsibilities for security.
· Engage and promote the process at a senior management level.
· Capture signatures of acceptance for understanding the requirements and specific roles and responsibilities.

1.2 Risk Management

· Using this guideline and other relevant industry best practice conduct an initial review of activities. Involve management and key stakeholders to identify all potential security related risk.
· Engage a studio or producer approved third party to assist in the assessment process and implementation of controls.
· Ensure management reviews are conducted periodically or when changes in content related activity occur.

1.3 Compliance

· Review procedures, practices and implementation to ensure ongoing compliance with this guideline and security requirements.

2 PERSONNEL AND RESOURCES / PRODUCTION OFFICE

2.1 Personnel and Resources

· Appoint an individual to be responsible for project and content security.
· Ensure they have suitable skills, capabilities and knowledge.
· Define roles and responsibilities for content security and asset protection. Document them.
· Ensure personnel security procedures and practices are implemented and that they are understood by all personnel.
· Appropriate background screening will be conducted where required.
· Confidentiality and non-disclosure agreements should have been signed and retained prior to project commencement. These should be maintained for changes in resources for the projects duration.

2.2 General Guidelines

· All General Content Security Guidelines listed in Section 8.1 below also apply to the Production Office, as well as all members of the crew and cast, where relevant.

2.3 Production Office

· Production Office is responsible for secure distribution and storage all start-up paperwork documents, signed agreements and other confidential production documents.
· Any assets located with the Production Office, especially those that store content (camera cards, drives, etc.) or other confidential Intellectual Property (scripts, budgets) should be securely stored in areas protected by security camera coverage, with limited access, as determined by the producers.
· Access to vaults, safes, or locked filing cabinets should be limited, to those personnel as approved by the producers.

2.4 **Non-Disclosure Agreements / Social Media Awareness / Etc.**
· Production Office responsible for production documents to be signed and returned by all production hires, including Non-Disclosure Agreements (NDA), Code of Ethics, Social Media Awareness, General Content Handling Guidelines, as determined by the producers and studio. · All crew members, background extras, day players, other members of the cast, and visitors should sign agreements to not photograph or otherwise share confidential information to friends, family, co-workers, or on Social Media websites or apps. This information includes but is not limited to, set locations, plot lines, actors, characters, etc. · Social Media websites include but are not limited to Facebook, Twitter, Instagram, Vine, LinkedIn, Pinterest, Tumblr, Vimeo, Google+, IMDB, OnLocationVacations, and more.
2.5 **Personal / Mobile Devices**
· When not in immediate use, personal / mobile devices such as iPads, iPhones, Android phones, laptops, tablets, set-top computers, that store sensitive production content, or other confidential Intellectual Property should be securely stored, protected with complex passwords, cable locked, and have remote tracking and disabling software enabled, and stored in a vault, safe, or locked filing cabinet.
2.6 **Cloud Storage / Collaboration Technologies**
· Production members should use studio approved file storage and collaboration technologies, instead of using consumer grade solutions (ie, DropBox, Google Drive, SkyDrive, etc., for storing or sharing sensitive files and content. · Content should be encrypted at rest. · User rights should have the ability for the Admin to control and restrict rights, and disable access remotely. · Where possible, content should be watermarked and/or spoiled to idenify the user.

2.7 **Security Systems**
· Security Cameras should be utilized at key entrances and exits, as well as areas with safe / vaults / locked filing cabinets that store Audio/Visual content or other confidential Intellectual Property, that is maintained for 90 days. · Entrances and exits should be alarmed, and remotely monitored by either a trusted third party security company, or by designated members of the production. · Authorized members of the production with access to enter Production Office after hours should have their own individual access code. · Access codes should be changed in the event as members of the production office end their employment, or are otherwise discharged from the production.
2.8 **Change Control**
· Security access codes and system passwords should be changed in the event as members of the production office end their employment, or are otherwise discharged from the production. · Physicals keys should also be collected, and locks changed on areas that store sensitive content and confidential Intellectual Property.
2.9 **On Set Visitation Policy**
· All on-set visitors should be pre-approved by the Producers, should have signed an NDA and Social Media Policy. · Further, the Production Office should verbally confirm the Social Media Policy and On-Set Photography Policy. · Visitor badges should be issued, then returned and accounted for by the Production Office at the end of the day. · On-set visitors should be escorted to and from the set. · All Personal / Mobile Devices should be silenced, powered off, or stored in the Production Office until afterwards.
Incident Escalation
· All members of a production should be aware of any unfamiliar person on set, and notify security if they do not have visible Visitor ID. · Any member of a production cast or crew should contact security if they witness anyone on set recording video, audio, or images with a camera, phone, tablet, or other recording device.

3 ASSET MANAGEMENT / CAMERA MEDIA

3.1 Administrative Controls

· Define asset management roles, responsibilities and handling procedures with segregation of functions where necessary, ensuring security measures are proportionate to risk.

3.2 Asset Controls

· Implement an effective process for asset management and tracking.
· This should be capable of providing an auditable chain of custody for content related assets and blank media.
· Consider the use of a register that that documents the time/date of creation/registration, current location, movement and final destination or destruction with suitable retained records should they be required.

3.3 Asset Receipt and Identification

· Ensure that all content related assets and blank media received are; logged into the register, uniquely identified and securely stored.

3.4 Secure Asset Storage and Reconciliation Controls

· Provide adequate physical storage and logical controls for assets when left unattended. See physical and IT security sections for more detail. Implement and maintain an inventory count procedure for content related assets and blank media.
· Where possible use independent personnel to conduct checks to ensure integrity is maintained.
· As a minimum keep records for the duration of the project.
· Report and investigate discrepancies and consider the need to escalate notification to management and content owners.

3.5 Asset Re-call Procedures

· Define a process for the recall of content related assets booked out.
· Give someone the responsibility to manage the asset register.
· Respond immediately and investigate any failure to return or loss of any asset.

3.6 **Control of Blank Media Materials**
· Treat blank media/blank media as an asset as it can be used to remove or transfer content without authority. · It should be; logged onto an asset register, identified upon receipt, secured and handled in accordance with work instructions. Blank media other than that registered should be prohibited from site. · Treat blank media as you would a storage device by implementing checks and controls.
3.7 **Transportation of Assets**
· Define procedures for secure transportation of content related assets (tapes drives film etc...), ensuring that records are retained within the asset register and that any 3rd parties have appropriate insurances. · Only use approved and appropriately screened members of production staff, runners and couriers. · Document the process for any Runners and Couriers and circulate to relevant personnel. · Consider the use of security seals and encrypted storage. Implement advance notification processes for receipt of content. · Packaging should be plain and non descriptive and should not contain title or sensitive project information.
3.8 **Destruction and Recycling**
· Define destruction and recycling procedures for content related assets. Document destruction and keep records for the duration of the project.
3.9 **Camera Media Handling**
· The Digital Imaging Technician (D.I.T.) should ensure that camera media is tracked at all times, whether it is on set, in the camera truck, production office, or vendor / dailies processing lab. · Camera media includes but is not limited to camera cards, hard drives, shuttle drives, Compact Flash (CF) drive, SxS card, SSD, Codex box, "Shoebox", "Media Vault", Cinestation, tape, disc, SAN, LTO, or recording deck. · Ensure that all content related assets and blank media received are; logged into the register, uniquely identified and securely stored. · Camera media should be taken from camera / on set to the Camera truck for back-up, transfer, and storage by the person designated by Digital Imaging Technician (D.I.T.).

3.10 **Camera Media Re-Use**
· Camera media should be securely stored and tracked until Post Production / Editorial has viewed dailies and camera logs, and authorized the D.I.T. to wipe and prep camera media for re-use.
3.11 **Shipping Drives to Vendor**
· AV content (dailies) sent out to dailies vendor should be stored and transported on shuttle drives that are encrypted and password protected, and in locked case, with tamper resistant packaging, with the driver / courier not having access to the key. · Materials should be packed securely using plain packaging, non-descript labeling and withhold any title/project information. · Shuttle drives sent out to vendor should be securely held and returned during normal production shooting hours.
3.12 **Unauthorized Back-Up Copies**
· No unauthorized back-up copies of the AV content (dailies) should be made without approval of the producers / studio.
3.13 **Reconciliation of Camera Media**
· All camera media should be reconciled at the end of the production, and all AV content securely deleted prior to return to rental company or for asset storage.
3.14 **Video Assist Cart**
· Video Assist Cart should utilize encrypted and password protected hard drives. · Video Assist Cart should be secured after hours inside locked equipment truck, with cable locks to secure cart and hard drives. · At end of production, at a time designated by the producers, all Audio-Visual content should be securely deleted from all hard drives, and the hard drives wiped and reformatted.

3.15 **On-Set Streaming**
· If approved for on-set streaming of dailies footage, content should first be ingested from the camera media onto a local server, that is both encrypted and password protected. · Dynamic visible user name burn-in should be added as content is streamed to iPad / tablets. · Files should be transcoded in a h.264 format with "Property Of …" and other appropriate spoilers burned in base video. · All iPads / tablets should have their Unique Device ID (UDID) registered in advance, with client app installed prior to set visit, with active ability to remotely track, lock, and wipe devices. · Download should be prohibited, and streaming should originate from a private WiFi network that is password protected, from a limited range Wi-Fi router. · The SSID (Service Set Identifier) should not be broadcast, preventing the name of the private WiFi network from showing up on a scan. · Dynamic visible user name burn-in should be added as content is streamed to iPad / tablets. · Audio-Visual content should be be securely deleted from hard drives once the content is securely at the dailies lab, backed up to LTO, check-sum verified, and deliverables complete. · The cart used to store, transcode, and stream Audio-Visual content should be secured as with the Video Assist Cart.

4 PHYSICAL SECURITY

4.1 Secure Perimeters

· Define within a security plan, what physical security controls are in place and how these are monitored.
· Brief staff accordingly on a need to know basis.
· Apply multiple layers of protection around the perimeter.
· Consider use of CCTV, automated access control, key controls, visitor procedures and perimeter intruder detection systems (PIDS).
· Utilize existing site controls wherever possible and consider the need for physical security upgrades prior to project commencement.
· Where third party controls are utilized ensure protocols for use and access to data is agreed within any contract or a written agreement prior to project commencement. Consider the need for nondisclosure or confidentiality agreements.

4.2 Securing Internal Areas

· Consider the sensitivity of production activities and the workflow.
· Create secure zones. Physically protect, monitor and restrict access to the production environment and all storage areas as necessary. Do this on a basis of need rather than convenience to reduce risk.
· Identify the requirements for any enhancement or increase in physical security where content is to be created, handled or stored.

4.3 Use of Guards

· Consider the value of deploying guards according to the level of risk, access to resources and the availability of alternative controls.
· Where existing facility or third party resources are used ensure security requirements for third parties are met, including NDA non-disclosure and suitable back ground checks.
· Review and/or create suitable assignment instructions maintain and check agreed activities are maintained.

4.4 **Searches**
· Define a search policy for the project · Consider the roles to be undertaken and the locations of the activity. · Link this to requirements for authorizing and prohibiting storage devices, mobile devices, removable media and blank media within the production areas. Consider the need for permanent and/or random searches. · Implement according to risk and activity. · As a minimum a search procedure “for cause” (in the event of incident or suspected unauthorized act) should be in place.
4.5 **CCTV**
· Ensure effective deployment of CCTV at points of entry and egress to a site and any designated internal secure areas. · Consider the need to extend coverage where content is handled or transferred without supervision or other corroborative control such as searches. · Define or integrate local procedures for CCTV. Ensure access to third party systems is agreed and that images are retained for a minimum period commensurate to the activity being monitored and risk to content. · Recommended retention periods for perimeter controls should exceed 30 days and the monitoring of internal locations should be extended.
4.6 **Access Control Key Controls and Automated Technology**
· Ensure effective deployment of access control and/or key controls at points of entry and egress to a site and any designated internal secure areas. · Define or integrate local procedures for access control. · Retain automated access control logs for the duration of the project.
4.7 **Intruder Detection Systems (Alarms)**
· Ensure effective deployment of IDS at points of entry and egress to a site and any designated internal secure areas. · Define or integrate local procedures for zoning and the responsible use of key codes. · Retain access activation logs for the project duration.

4.8 **Check Visitor ID**
· Security guards should be cognizant of all visitors on or near the set, and should make sure they have proper visitor badge identification. The producers should have a clearly defined search policy for the project.
4.9 **Key Assets / Props / Costumes / Equipment**
· Areas holding key assets such as props, costumes, equipment, computers, or other valuable assets should consider use of CCTV, automated access control, key controls, visitor procedures and perimeter intruder detection systems (PIDS). · Utilize existing site controls wherever possible and consider the need for physical security upgrades prior to project commencement.
4.10 **Camera Truck**
· Camera truck should secure all devices used to store or process Audio-Visual content, including a safe or locking vault to store camera media, hard drives, laptops, or any other device used to store or process Audio-Visual content. · Camera truck should be kept in a secure location, locked, and where possible with alarm and security camera coverage.

5 IT SECURITY

5.1 Information Security

· Define and develop IT security plans. Prior to project commencement consider and assess the need for the following controls:

· Control of authorized and prohibited devices and software
· Inventory requirements for authorized devices and software
· The secure configuration and segregated use of hardware and software on production networks
· Basic requirements for vulnerability assessment, malware controls and application/software security updates
· Public facing boundary defenses to include properly managed firewalls, DMZ and Intrusion detection
· Secure server and device configuration
· Logical and physical segregation for production networks
· Securely engineered networks and end point security controls for all devices handling content
· Wireless router and device controls
· Network access controls to include port, protocol and restricted/controlled access to services
· Securely managed administration of production networks
· Managed, monitored and controlled logical user access to content within production networks
· Logging enabled, monitored and securely stored
· Process for incident response and the capture of evidence"

5.2 Acceptable Use

· Define the acceptable use for IT systems and devices; include use of the production network, authorized use of devices and restrictions on access to web based services. Capture individual's acceptance of policy.

5.3 System Administrator and Elevated Privilege User Accounts

· Authorize and define requirements for the administration of production networks. Prevent the use of administrator accounts for non-administrative functions. Log and retain details of administrator actions for the duration of the project.

5.4 **System Basic User Accounts**
· Consider the level of access required to content and restrict access to production networks accordingly. Use a policy of authorized and need to have only. Restrict file access and sharing using appropriate configuration controls.
5.5 **Password Management**
· Define a Strong Password policy for all devices and workstations containing or accessing media content: · At least eight characters long · Does not contain any user name, real name, nickname, company name or identifiable number. · Is unique and not used elsewhere. · Does not contain a single complete word. · Contains one from each of the following four categories; Upper Case, Lower Case, Number, Character Changes should be significantly different from previous passwords. · Password changes should be made every 30 days. · Devices should be set to auto log out after five minutes.
5.6 **Authorizing Third-party Access to IT Systems**
· Define third-party access policy and procedures. Only approved devices should be connected to networks or devices where media content is stored or accessed.
5.7 **Removable Media**
· Include authorized removable media within an approved device register. · If possible identify approved devices using hologram or other non-descriptive marking. · Prohibit the use and possession of non-approved devices where content is handled, created or stored. · Use end point security software and/or disable ports and peripheral device writers at source to prevent unauthorized connection of non-approved devices. Treat blank media as a removable media asset and place it on a register. Control access and use. Complete inventory checks.

5.8 **Mobile Device Management**
· Establish, implement and maintain a mobile device acceptable use policy. · Complete an approved device register recording authorization to possess devices where content is handled, created or stored. · Where personal items capable of content transfer or storage are permitted into production areas this should be authorized by management, documented and monitored. · Persons authorized to carry personal items of this nature should be advised of the risk and consequences of unauthorized use of the device and that they may be subject to search and additional checks and controls.
5.9 **Wireless Networks**
· Define a wireless network policy to include acceptable use. · Deny the use of wireless on production networks. · Implement strong user and password authentication for Staff and any guest networks. Implement encryption WPA2 minimum standard. · Prohibit the transfer of feature content via wireless networks.
5.10 **Environmental Security Controls**
· Physically secure server locations monitor and restrict access. · Physically secure systems and hardware to prevent misuse and configure so as to prevent any circumvention of secure connections.
5.11 **Network Monitoring**
· Establish how network traffic is to be monitored retain event logs for the project duration.
5.12 **Access Controls**
· Establish policy and process to identify and control access using secure configuration and authentication.
5.13 **Remote Access**
· Establish policy and process to identify and control remote access requirements using dual factor authentication for VPN or equivalent.

5.14 **Change Management**
· Appoint an administrator responsible for policy and process to manage changes
5.15 **System Documentation**
· Document and maintain a basic network diagram.
5.16 **Networks**
· Securely configure and segregate internal and external networks. Isolate content networks from no-production networks.
5.17 **File Transfer Management and Data Storage**
· Establish policy and processes for all file transfer and encryption technologies. · Only use studio approved hardware and software for content transfer. · Apply secure configuration and administration controls. · Retain log files for all content tranfers. · Content within all data storage locations should be kept physically secure when unattended. · Use approved hardware for storage systems and segregate where possible. · Use approved encryption methods for transfer and storage. · As a minimum use AES 128 Bit Encryption.
5.18 **Firewall Management**
· Correctly configure firewalls to deny untrusted incoming traffic. · Implement firewall rules to deny all outbound traffic by default. · Control and monitor outbound traffic using secure configuration controls to prevent loss of data/content and protect network integrity. · Review configuration regularly during the project.
5.19 **Vulnerability Management**
· An anti-virus policy shall be documented and implemented. · Servers and workstations are protected. · Implement a patching regime for servers, workstations and security barriers.

6 TRAINING AND AWARENESS

6.1 Training and Awareness Needs

· Establish anti-piracy and security awareness briefings.
· Record details of persons completing the awareness package.
· On projects of a long duration refresh awareness during key phases of production (ie, after the Director's Cut or Picture Lock).

6.2 Kick-Off Meetings

· Include a Content Security discussion at key Production and Post-Production kick-off meetings, to make key members of the production team aware of risks, and studio expectations, for protecting the Intellectual Property and Audio-Visual content.

6.3 Start-Up Paperwork

· Producers and Production Office responsible for requiring all cast and crew members to sign agreements to not photograph or otherwise share confidential information to friends, family, co-workers, or on Social Media websites or apps.
· This information includes but is not limited to, set locations, plot lines, actors, characters, etc.

7 INCIDENT MANAGEMENT AND RECOVERY PLANNING

7.1 Incident Management and Recovery Planning

· Establish a process for reporting and responding to a security incident Establish a basic continuity and recovery plan
· Review effectiveness
· Record details of persons completing the awareness package.

7.2 Geographic Separation

· All Audio-Video Content, including dailies, rough cuts, and VFX shots, should have back-up copies, with geographic separation of original version and back-ups.
· A back-up copy of all Edit Decision Lists (EDL) from editorial (Avid, Final Cut Pro) should be maintained at all times, for retrieval and restoration of project.

8 EDITORIAL / DIGITAL WORKFLOW

8.1 General Guidelines

The following requirements outline the fundamental guidelines has been developed for safeguarding the content handled during Production and Post Production. The Post Production workflow and content created during this phase are unique and the controls for protecting this material have been specifically put in place for it.

a	Closed Set: Maintain a “closed set” environment. If people do not need to have visibility/access to content, they should not be permitted in areas where content is handled. If people will have visibility/access to content, they should sign the applicable non-disclosure agreement (NDA).
b	Complex Passwords: Use complex passwords for all systems, programs and devices that require a password. Complex passwords are at least 8 characters, consisting of upper- and lower-case letters, numbers and symbols. An example is: P@ran0iD. Passwords should not be shared. Passwords should be changed at the start of every show.
c	Restrict Internet Access: Internet access is never allowed on any systems handling and/or storing content. You should unplug Internet cables and/or disable wireless access on Production Networks.
d	Encrypt Data : If thumb drives or external hard-drives are used, they should be, at minimum AES 128-bit, encrypted and securely stored when not in use. Complex passwords/phrases are required and should be sent separate from the device.
e	Physical Security: Areas where content is stored or handled should be kept as physically secure as possible. This requires doors to be locked when staff is not present, physical materials to be locked in safes/cabinets/vaults, and if possible security camera and swipe card systems installed covering sensitive areas.

8.1	**General Guidelines Continued**
f	Secure Electronic Transfers: All electronic transfers should be conducted via studio approved transfer technology (Aspera, Signiant, Sohonet, etc.). Content may never be sent over email or uploaded to a system that has not been approved (e.g. YouSendIt, FTP, AIM, etc.). If a vendor requests to use an alternate system, Content Security should be contacted to have these systems reviewed.
g	Secure Physical Deliveries: All materials being sent physically (e.g. tapes, drives, film, etc.) should be sent using a production employee, studio employee or an approved courier/freight service. Materials should be packed securely using plain packaging, non-descript labeling and withhold any title/project information.
h	Appropriate Spoilage: Unless otherwise approved by the studio, "turn-over copies" should have unique spoilage specific to the recipient.
i	Approved Vendors: If requested by the studio, the production shall endeavor to use only vendors who the studio has conducted security reviews and approved vendor to handle content.
j	Principle of Least Privilege: Do not send content to people who do not absolutely require content. Content will only be provided to persons absolutely requiring access to our materials. When content is provided, it should follow the above guidelines for delivery, spoilage and handling.

8.2 Digital Workflow

The Producers, Post Production Supervisor, and the Digital Imaging Technician (D.I.T.) should create a detailed Digital Workflow, to be approved by the studio, to include the following areas:

· Method of Digital Acquisition (camera, camera media)
· Processing of dailies On Set vs. Near Set vs Lab
· Application of color correction / Look Up Tables (LUTs)
· Ingesting Audio-Video content to local SAN or hard drive for creating deliverables
· Check-sum verifications
· Transcoding to dailies and editorial media specs
· Syncing of audio and video
· Digital or physical delivery to studio executives, editorial or VFX
· Back-up copies to LTO or other formats
· Additional check-sum verification of SAN or hard drive to LTO or other format
· Archival back-up copy with geographic separation
· Process for how long to hold camera media for re-use
· Determine who authorizes wiping of media for re-use after editorial and camera department review content against camera reports

8.3 Burn-ins / Spoilers / Watermarking

· Burn-ins / spoilers / watermarking should be used to the highest degree possible without frustrating the intended business purpose.
· Only use studio approved solutions for sending, receiving, viewing, collaborating, or transforming content.
· Apply unique markings and make identification specific to the recipient.
· Show the name of the facility/company, recipient initials and Dub date.
· Use assigned project alias to label media.
· Consider the need to de-saturate media intended for vendor dissemination.
· Consider the need to physically secure media such as DVD and tape before distribution. (See section 3.7)
· Do not leave physical media unattended at any time. (See section 3.7)

8.4 **Online Screeners / Media**
· Only use studio approved delivery applications. · Login credentials are specific to the recipient and are not to be shared under any circumstance · Pre approved burn-ins should be applied. · Download facility should be approved by studio.
8.5 **Vendor Duplication**
· Editorial and studio should be responsible for media output during post production. · For media that has bespoke technical requirements use studio pre-approved vendors only. · Such content is considered high security and can only be approved by studio authorized staff or their designees
8.6 **Screenings**
· Do not send clear media without ADVANCE approval of studio · Media burn-ins are mandatory unless authorized. · Editing room staff should be present and will be responsible for the handling and transport security of content to prevent unauthorized duplication, transmission or access. · Should screening of clear content be required, the studio approved screening room should be used.
8.7 **Editing Rooms**
· Editing Systems should be configured to prohibit internet access. · All drives should be scanned for viruses and malware prior to attaching to storage devices or ingesting content onto production network · Content should be transferred from a centralized data I/O (input/output) station (using approved encrypted transfer technology), and securely deleted from the station once delivery has been confirmed. · Devices used for e-mail or other access to the internet should never contain user names or passwords for systems with access to content, and should not be used to download, transfer, receive, or otherwise access sensitive content. · Production network storage devices (Isilon, ISIS, SAN, Xtore, etc.) should be kept in well ventilated and temperature controlled environments, with CCTV coverage where possible, with keycard access where possible, and locked when not under immediate supervision of the editorial staff.

9 SCRIPT HANDLING

9.1 Development & Pre-Production

· Scripts should be distributed digitally via an access control system, unless a physical copy is otherwise approved by the Producer.
· All Scripts should be watermarked with recipient's name.
· Digital Script security settings should prevent printing / copying / forwarding.
· Digital Scripts should be set to "expire" and auto-delete from recipient devices after a time frame determined by Producer.
· Physical scripts should never be unattended, should be kept locked up unless in immediate use, and shredded or returned to the Producer after an agreed upon timeframe.
· Scripts should be distributed only to the intended recipient.
· Scripts at table reads will be watermarked, signed for, collected afterwards, and either shredded or locked away securely at discretion of the Producer.
· All elements of the script including storyline, locations, characters, props, dialogue, etc., are covered under Non-Disclosure Agreements, and should not be discussed with anyone outside the relevant members of the production (unless authorized by the Producer), including friends, relatives, and all Social Media outlets.

9.2 Production (Scripts & Sides)

· Scripts & Sides should be distributed digitally via access control system, unless physical copies are otherwise approved by the Producer.
· All Scripts & Sides should be watermarked with recipient's name
· Digital Script & Sides security settings should be set to prevent printing / copying / forwarding.
· Digital Scripts & Sides should be set to "expire" and auto-delete from recipient devices after a time frame determined by Producer.
· Physical Scripts & Sides should never be unattended, should be kept locked up unless in immediate use, and collected at the end of the day to be either shredded or locked away securely, at discretion of the Producer.
· Scripts should be distributed only to the intended recipient.

9.3 **Personal / Mobile Device Policy**
· Personal / Mobile Devices include Pads, Tablets, Laptops, MacBooks, iPhones, Android Phones Set-top computers, and other such devices that store content or other confidential Intellectual Property · When not in immediate use, these devices should be securely stored, protected with complex passwords, cable locked, and have remote tracking and disabling software enabled, and/or stored in a vault, safe, or locked filing cabinet. · Personal / Mobile Devices should be configured with a complex password where possible, with minimum 4-digit non-consecutive and non-repeating PIN # where applicable. · Personal / Mobile Devices should be configured to lock-out after 5 unsuccessful log-in attempts. · Personal / Mobile Devices should be set to track / lock / delete contents remotely. · Personal / Mobile Devices back-up data should be encrypted. · MacBooks and PC's should enable FileVault / FileVault2 security settings or other technology as approved by the Producers or the Studio.