Film & TV Production Security Guidelines

Appendix B – General Guidance Summary

Developed and Maintained by CDSA's
Production Security Working Group

www.CDSAonline.org

(RETURN TO TABLE OF CONTENTS)

INTRODUCTION

AUTHORS

These Film & Television Production Security Guidelines have been prepared by the Television Security Working Group of the Content Delivery and Security Association (the CDSA). The group is made up of security executive representatives from many of the major studios and film and television producers, PGA members, and members of the CDSA's board of directors.

PURPOSE

We have worked to create an industry security standard for preventing and otherwise defending against the unauthorized or unintentional access to intellectual property in this era of evolving security threats, particularly cyber threats, which requires technical controls and effective security management processes.

Additionally, we have worked to create a standard that crew can learn and apply on any production for any producer. Every production will be different, will have different priorities and different resources. These guidelines are recommendations. Each production will need to determine how they implement them.

This General Summary does not address every guideline but includes those that provide the broad overview. *(The paragraph numbering aligns with the full Production Security Guidelines and therefore is not continuous.)*

TARGET AUDIENCE

The guidelines are dense and it is not expected that all producers and crew will read them cover to cover.

We recommend establishing a Security Team made up of representatives of all the production departments. Their role will be to lead the entire production team in good security practices. We also recommend the Security Team should read these guidelines cover to cover. Even those guidelines which won't mean a lot to them individually or in their particular job role.

Understanding the whole of the security best practices, how they work together, build on each other, depend on each other, use similar functions and rules, relate the physical to the virtual spaces and

assets, will enable the security team to better plan for and promote smart secure practices on the production.

This General Guidance Summary distills the full guidance down to the core recommendations which should be understood and implemented by the **production management team**.

ORGANIZATION

PEOPLE

All security begins and ends with people. Hence the first chapter is about the individuals: their individual responsibilities and the production's responsibilities managing individuals' engagement, training and access.

PHYSICAL

Protecting the physical access to people and physical assets including physical equipment storing virtual assets is a key component of overall security.

ASSETS

Assets are the subject of the security measures and come in many forms, listed in a general order of increasing volatility:

- Facilities
- Equipment
- Paper
- People
- Media
- Data

They also come in many different types of importance such as:

- Uniqueness to the production
- Cost to replace
- Value to marketing
- Exposure to regulations

Assets are plugged in the middle of the guidelines as they are the bridge between the physical and the virtual spaces.

VIRTUAL-DATA

The greatest challenge to production security is the management of data which includes the largest number and likely most valuable assets despite their lack of tangibility.

It is important to note that the security measures used for the virtual space have equivalent measures in the physical space, which can be used as references when mapping out the design and plan for the production's data security.

Several sections in this chapter will be directed specifically at the IT professional(s) responsible for implementing, building, and monitoring the production's digital data workspaces. These sections will provide for the production's Management and Security Team a checklist to review with the IT professional(s) and to budget for.

PLANNING FOR SECURITY AND RESPONSE TO BREACHES

While every production is unique and needs its own plan appropriate to its exposure and resources, these guidelines will provide a checklist to review, consider and adapt as appropriate, when planning for the who, how, what, when, where, why, before, during and after of any potential breach.

I. DEFINITIONS

ASSETS

Content: the intended product of the production and all its iterations from concept to completion. May be used interchangeably with Digital Asset.

Digital Asset: an asset that exists in digital format, examples being:

- Documents – scripts, sides, treatments, callsheets, production reports, financial reports, contracts, etc.
- Media files – set designs, concept designs, vfx assets, dailies, cut scenes, audio clips, etc.
- Database data and metadata – financial records, editorial EDLs, vfx metadata, etc.
- Electronic communications - emails

examples of data asset formats being:

- Documents – docs, spreadsheets, pdfs, etc.
- Media files – mp4, jpeg, mov, any design files such as visual effect layers and assets, and set design CAD files, etc.
- Database data and metadata – data stored in accounting system, Filemaker, Avid, Shotgun, Stornext etc.
- Electronic communications - emails

Physical Asset: an Asset that that can be touched, examples being:

- Costumes

- Props
- Office equipment
- Computer equipment – Servers, Networking, Desktops, Laptops, Portable Drives, USB drives, Mobile devices, etc.
- Raw or exposed stock and blank or recorded media – tapes, disks, drives
- Paper documents – letters, executed contracts, payroll records, etc.

Work Product: Items created while on production and therefore the property of the production company, examples being:

- Correspondence
- Photography
- Designs
- Templates
- Reports
- All Content
- All Assets

Intellectual Property: All assets generated by the production related to the making of the Content, examples being:

- All products of work-for-hire contracts
- Pitch, if purchased
- Treatment
- Synopsis
- Bible
- Scripts
- Casting lists
- Designs
- Concept art
- Research
- Samples
- Costumes and Props manufactured by production
- Sets and Set Decorations manufactured by production
- Unique tools developed and/or manufactured by production
- Versions in progress
- Continuity photos
- Rehearsal photos or footage
- Sound recordings
- Sound samples
- Image recordings
- Edited selections
- Edited cuts

- Un-composited picture or sound layers
- Composited picture or sound layers
- Rejected versions of all the above
- Out-takes
- Unused footage or sound
- And: the release version(s) of the Content

Regulated Information: Information for which mismanagement, mishandling, or exposure would result in regulatory driven legal repercussions, examples being

- Personally identifying information, "**PII**", are any pieces of information that can be combined to identify a unique individual, examples being:
  - name,
  - address,
  - tax or government ID number,
  - phone number,
  - email address,
  - IP address,
  - Physical location
  - GPS location,
  - photo,
  - family member

  which is subject to the EU GDPR and the many State and other regulations protecting personal identifying information.

  Examples of documents which include PII are:

  - Call sheets
  - Contracts, deal memos, waiver forms
  - Emergency contact forms
  - Travel memos
  - Payroll start forms
  - Time cards
  - Crew and Cast lists
  - Vendor contact lists

- Health related information (insurance, medical report, prescription, etc.) which is subject to "**HIPAA**".
- Financial information (credit card number, banking details, salary terms, corporate financial data, etc.) which is subject to "**PCI"** and/or Sarbanes-Oxley ("**SOX**").

Confidential Information with business competitivity value and/or potential anti-trust exposure, examples being:

- bids,
- estimates,
- budgets,
- schedules,
- vendor contracts, etc.

HACK

Unauthorized view, access, copy, print, share, transfer, theft, corruption or deletion of data assets.

HACKER

A person who views, accesses, copies, prints, shares, steals, corrupts or deletes data assets without authorization.

There are many types of hackers:

- Not a User – see "User" below
- Felons – actively seek to hack
- Opportunists – take advantage of the opportunity to hack
- Careless people – ignore or disregard access policies for convenience
- Victims of hackers – aid hackers by falling victim to phishing or other attacks and then provide unauthorized access to data
- Uninformed – do not know the access policies

LEAST PRIVILEGE PRINCIPLE

In this principle, a person should only be granted the minimum access necessary to assets, information and resources to perform his/her job duties. Examples being:

- Editing rooms are restricted to those authorized to see cut footage only.
- The dailies screening is restricted to those authorized to see dailies.
- Only payroll accounting staff may access HR files, all others have no access except to their own payroll documents.
- The design and drafting spaces may have access restricted to the director, producers, and key personnel directly involved with the design and planning of the project. Personnel uninvolved with designing and planning, e.g. set crew, general office staff, etc. may be unauthorized to enter.
- Folders within a file sharing system may have access limited to specific user groups and file permissions.
- Cloud applications may have access and privileges (view, annotate, edit, copy, share etc.) limited to specific user groups.

NETWORK

A network is a group of connected computers, devices, and systems between which data may flow or be accessed. There are numerous types of networks:

- *LAN – Local Area Network*: connected computers within a single building or geographic space (e.g. production office or base camp). LANs may be hardwired via ethernet or wireless via WIFI.
- *WAN – Wide Area Network*: connected computers which are geographically distant and connected via communications services (e.g. telephone, cable, internet or VPN).
- *VPN – Virtual Private Network*: a secured data tunnel to connect to the network.
- *WIFI Network*: a wireless LAN.
- *Restricted Access Network*: a network which has strict limited access privileges suitable for highly confidential data.
- *General Access Network*: a network which is accessible for general office operations and access to the internet restricted to production personnel.
- *Guest Network*: a network provided for visitors and guests which provides internet access only.

PERIMETER

The border between what is controlled and secured by the production and what is not. The perimeter may be physical or virtual.

SECURITY TITLE

Pseudonymized title used to maintain secrecy of project in production. Security titles may also be called Temporary or Working Title, Alias or Code Name.

THIRD PARTY PERSONNEL & CONTRACTORS

The terms “third-party personnel” and “contractors” can be used interchangeably for persons employed by a vendor or loan-out company which is providing their services to the production.

Generally, the difference inferred in this document is that a third-party employee is managed wholly by the third-party vendor, whereas a contractor may be partly or wholly managed by the production.

In most instances where one group is referenced, the policy may equally apply to the other.

USER

A person who accesses data via a digital identity. Generally, a user is an individual who has been provided a username and password to access data via a network, application, cloud service, or email etc.

USER GROUP

A set of users grouped based on shared criteria, e.g. department, job role, responsibility, etc.

VISITORS

Visitors include guests of production personnel, representatives of production vendors, delivery and courier services, etc. Individuals who access production facilities but have no direct involvement in the production.

WORK PRODUCT

Work product is the result of contracted labor or services and includes research, designs, prototypes, final assets, paperwork, and correspondence (paper and email). Work product is an asset of the company, not of the individual creator.

(RETURN TO TABLE OF CONTENTS)

II. PEOPLE

2.1 INDIVIDUAL RESPONSIBILITY

2.1.1 SECURITY MANAGEMENT TEAM

A team of individuals should be specifically assigned security oversight responsibilities, the ***"Security Team"***. The team should include individuals who oversee physical, creative and data management activities. All areas of security overlap and the team should view each other's roles as interdependent.

All persons involved on a production are members of the security team. Security policy and procedure training should be provided to everyone. But some individuals need to be identified as specifically responsible for steps in the workflow such as a department, facility, process or type of equipment. Provide more in-depth training for these key individuals who will act as security stewards.

There is a parallel to safety policy implementation which assigns particular safety supervisory responsibilities to managers, assistant directors, special effects and stunt coordinators etc.

The Security Management Team should meet periodically to develop risk assessments and business continuity plans particularly as they relate to hand-offs in the workflows from one steward's purview to another's.

2.1.2 ALL CREW AND CONTRACTORS

All individuals should be required to take personal responsibility to adhere to the security guidelines and best practices.

Each individual's responsibilities include, but are not limited to:

- Understanding and adherence to the production non-disclosure or confidentiality agreement.
- Wearing production ID at all times and in a manner easily visible to others.
- Identifying and/or recognizing assets and caring for them appropriately
- Being observant of the environment and the people and objects within it. If anything or anyone is suspicious, out-of-place or simply unidentified, take the steps to question, remove or to notify a person with the authority to do so. Examples:
    - Do not be polite and allow unidentified people to follow you through a secured door.
    - If you see someone without an ID and who you do not recognize on the set or within a restricted area, politely ask them to wear their ID where it can be seen or notify an AD, Locations, Security or other appropriate person of the unidentified individual's presence.
    - If you see an asset left unattended and at risk, notify its owner of its location (where?) and exposure (why?). If you are unable to locate the owner, take it to someone who will be able to find out.
    - If you see an entry left open, unlocked or unattended, close it, lock it or find someone to attend to it.
- Using only approved communication tools provided by production (e.g. email account, chat service, file sharing service.)
- Using only approved systems, services, applications, and devices (computers, smartphones, portable storage, etc.) when, where and how instructed by production.
- Storing work product appropriately according to production policies. Examples:
    - Props in the props lock-up.
    - Portable drives in a vault or safe.
    - Data files on the production shared storage.
- Accessing only appropriate work sites. Not entering restricted areas without authorization.
- Accessing only appropriate data (files, media, databases) as permissioned. If inappropriate access is made available in error, notify department head or IT to correct the access permission.
- Keeping all devices (computers, smartphones, tablets, etc.) secure with:
    - up to date versions of operating system, browsers and applications. (Most updates today are issued to patch security vulnerabilities, not updating a device turns it into a hacker target.)
    - encrypted (password protected)

    - loss protected with remote lock and/or remote data wipe: enrolled in the production's endpoint management program or, if not provided, enrolled in a "find my phone" service which offers remote lock and/or data wipe.
    - up to date anti-virus/anti-malware (including on Apple devices, they are not immune and if the virus or malware doesn't affect the device, it may be spreading the infection to others.)
    - enabled firewall
    - back-up to secure data backup service or secured drive.
- Vigilance against cyber hackers:
    - Checking the source before opening email or social media links and attachments.
    - Not providing confidential information via email or social media
    - Reporting spam, phishing or any suspicious communications.
- ***When uncertain about any policy or best practice, asking for guidance***.

2.2 ENGAGING EMPLOYEES & CONTRACTORS

2.2.1 BACKGROUND CHECKS, REFERENCES & CERTIFICATIONS

Determine which employee positions and third-party providers merit background and reference checks prior to commencing hiring.

Establish method - who performs checks and how (e.g. Security Services provider should perform background checks on supplied Security Guards.)

Check vendor references with studio security when available and/or if vendor is a facility managing content verify vendor's status on the Trusted Partner Network (TPN).

2.2.2 CONFIDENTIALITY

Non-Disclosure Agreements

Unless prohibited by law or applicable union or guild restrictions, all employees and third-party personnel should be required to sign Non-Disclosure Agreements ("NDA") or confidentiality agreements prior to accessing any confidential assets (e.g. scripts or production workspaces). The NDA should include language stating that disciplinary action may be taken if confidentiality is breached.

In lieu of separate agreements, non-disclosure or confidentiality provisions may be included as part of an employment contract.

Explain the terms of the NDA and what information, images, media etc. are considered confidential. Do not assume an employee's understanding of confidentiality or confidential information.

Provide a take-away copy of the non-disclosure/confidentiality agreement signed by employee or third parties separate from employment or services contract.

Social Media Awareness

Personal experiences, opinions and information related to pre-release content and related project activities including shooting location, plot points, spoilers etc. should not be shared to any social media platform, e.g. Facebook, IMDB, YouTube, or Instagram and personal sharing platforms such as personal Dropbox, iCloud or Smugmug, etc.

Personal experiences that occur within a restricted area such as on the set, in the editing room, in the art department may not be shared, no photos from anytime at work should be shared, personal photography within restricted areas is not allowed and may not be shared.

In instances when an orchestrated social media campaign is planned or underway, consult the person managing the campaign (e.g. Studio Marketing or Publicity department) prior to posting.

2.2.3 SECURITY REQUIREMENTS

Provide production security guidelines tailored to job roles.

Provide a take-away copy of the security requirements signed by employee or third parties separate from employment or services contract.

2.2.4 SECURITY AWARENESS TRAINING

Allow time when starting new cast and crew members or contractors for security awareness training. At a minimum verbally confirm their understanding of the production security guidelines and of the NDA in their agreement and provide take-away guidelines for them to keep. Include security awareness training as part of the daily hires sign-in procedure.

Security awareness should be a topic included at any “kick-off” or production meeting.

Security awareness reminders should be posted in key locations.

Post standard confidentiality agreement terms and reminders where employees, contractors and visitors will see them frequently.

Training and/or postings should give clear examples of inappropriate social media activities.

2.2.5 DAILY HIRES AND EXTRAS MANAGEMENT

The same policies and procedures should apply to all persons engaged by the production including those engaged for a single day such as daily crew, cast and/or extras.

2.2.6 EXIT PROCESS UPON COMPLETION OF SERVICES OR TERMINATION

Don't leave employee terminations procedures to chance. Make sure the production staff and accounting/payroll staff have clear actions to take and document, and persons to notify.

2.3 ACCESS CONTROLS

2.3.1 IDENTIFICATION

Proper use of photo IDs should be enforced for production crew and contractors.

Temporary IDs should be provided to guests and temporary hires.

2.3.2 SEGREGATION OF ACCESS AND DUTIES

Limit single person's direct and unilateral control of assets.

Duties should be segregated to eliminate overlap of job functions within the workflow where assets are controlled through several process steps.

Implement controls to provide secondary oversight and minimize risk of loss when multiple duties are assigned to a single person.

2.3.3 CONTRACTORS AND THIRD-PARTY PERSONNEL ACCESS

Third parties who require access to production premises or assets or, who create assets off-site should be provided the security policies and guidelines and required to adhere to them. (Additionally, see section *2.2 Engaging Employees & Contractors*; third parties handling production assets should be vetted for their security procedures such as via the Trusted Partner Network audit program.)

2.3.5 VISITOR SUPERVISION

Visitors should be accompanied at all times by an escort or their host. Visitors should not be left unaccompanied or supervised by persons unaware of the purpose of the visit.

(RETURN TO TABLE OF CONTENTS)

III. PHYSICAL – BRICK & MORTAR – SECURITY

3.1 FACILITY SECURITY

3.1.1. IDENTIFY PERIMETERS

Production perimeters are any areas where the production-controlled space meets public uncontrolled space, e.g. the doorway from the production office to the building common hallway, the perimeter of base camp, the stage doors on a shared lot.

When considering facilities and locations be sure to include the perimeter exposure including irregular access points (such as emergency exits, or unfenced areas) and the challenges to secure them.

Consider also the differentiations of internal perimeters - areas where all crew and guests may access versus restricted areas.

3.1.2 PERIMETER

After your people, the production perimeter is the next line of defense. Awareness of its location and weaknesses is a crucial step in securing the production.

Production perimeters should be secured against unauthorized entry.

Physical security measures should be commensurate for the location considering the external risks and the assets exposed.

3.1.4 SHARED FACILITIES - VENDORS

When booking facilities or services which will store, manage, transfer or transport physical assets, confirm the security policies in place are in line with the productions policies. Additionally, confirm their security standards and policies adhere to the MPAA best practices and the current status of their most recent security audits from the MPAA, CDSA or TPN.

As an alternative to the MPAA best practices, vendors who are not specific to the film & television industry should implement security policies based on the general standards ISO 27001 and 27002 series.

3.2 PHYSICAL SECURITY & SECURITY GUARDS

3.2.1 GUARD ASSIGNMENTS & AWARENESS

Productions should station security guards on site during working and non-working hours where appropriate based on environmental risk factors (e.g., blind access points, high traffic access points, general exposure to public access, crime rates, local police response times, etc.)

Security guards should be trained on appropriate production security policies regarding access privileges, e.g. ID badges, guests, use of personal devices, areas of differing access restrictions, times when access is more restricted, etc.

3.2.2 GUARD PATROL PROCEDURES

Security guards should regularly patrol the production perimeters and areas to monitor for suspicious activity. Recommended frequency depends on the size of the facility and the number of entry and exit points. Random routes and checks should be utilized to prevent easily identifiable patterns.

Remind crew not to distract guards and to co-operate with them to correct a detected breach of the perimeter.

3.2.3 GUARD AUTHORITY

Provide clear powers and limits of authority to security guards.
Examples:

- the power to prevent access to production areas to persons without proper identification, or the limited authority to escort those persons to a crew member authorized to provide production identification;
- the power to notify law enforcement in case of illegal entry or discovery of a theft, or the limited authority to contact the producer for instruction upon discovery of an illegal entry or theft.

3.3 FACILITY AUTHORIZED ACCESS

3.3.1 AUTHORIZED ACCESS CONTROL PROCEDURES

The rule of least privilege should apply to physical locations as well as access to information and content.

Clearly define for all production staff and contractors who should and should not access restricted areas. Put up signage identifying restricted areas. Design ID badges to identify approved access areas.

The daily Call sheet can be used as the instrument for defining the list of authorized individuals for the day and their appropriate physical access.

3.3.4 PHYSICAL ACCESS LOGGING

Productions should implement and maintain procedures to log access activity. The access log should be retained ensuring access to secure areas is monitored.

Keeping a history (log) of access to the production spaces and in particular to restricted spaces will seem burdensome until there is a breach and identifying who was where when will be essential to investigating the incident.

3.3.10 USE OF PORTABLE DIGITAL DEVICES WITHIN RESTRICTED AREAS

Use of recording, storage, or transmission features in digital devices (e.g., smartphones, tablets, USB thumbdrives, digital cameras, and laptops) in restricted areas should not be allowed.

No one can live without their smartphone! Successfully limiting smartphone use in sensitive areas (e.g. on set) is dependent on 'leadership by example'. The same rules and policies apply to all production staff. For those who need their smartphone or tablet to do their job, issue ID badges which clearly identify them as having been granted special permission to do so.

Any use of recording, storage, or transmission features in digital devices (e.g., smartphones, tablets, USB thumb drives, digital cameras, and laptops) in restricted areas should not be allowed.

(RETURN TO TABLE OF CONTENTS)

IV. ASSET MANAGEMENT

4.1 PSEUDONYMIZED SECURITY TITLE

4.1.1 USE OF ALIAS TEMPORARY TITLES

A Temporary title is often called the working title. It may also be called the Code Name, Alias, Security Title, etc. It is any title used in lieu of the commercial title of a project in order to protect

the anonymity of the project during its production and avoid drawing hacker, media, fan or other parties' attention.

When a Temporary Title is used, it should be used consistently on all asset (digital or physical) labels and within any documents.

The legal Title(s) are the release title(s) and/or the title of the material originally purchased or licensed to produce. There should be clear documentation to associate all assets labeled with the Temporary Title to the legal Title(s) as part of the chain of title evidence.

It is less confusing and more effective to use the alias on everything than to interchange using the real title and the alias.

Notify key contacts - studio, marketing, distributor - of chosen alias.

4.2 HIGH VALUE/CONFIDENTIAL SECURITY DESIGNATION

4.2.1 ASSET SECURITY DESIGNATION

There should be a clear production policy to designate "high security" assets based on their value, production content, regulatory or business confidentiality.

Err on the side of confidentiality and high value. More assets, particularly digital assets (media content, scripts, payroll records, bids and contracts, etc. plus call sheets, production reports, concept and design files, etc.) warrant "high security" treatment than one may think.

4.3 INVENTORY POLICIES

RECORDING CHAIN OF CUSTODY

Tracking and logging access, location, custodian(s) provides the place to begin any investigation relating to a loss. It may also serve as demonstration of best protection efforts in the case of losses of regulated information or business assets.

4.5 PEOPLE ARE ASSETS

4.5.1 SECURITY FOR THE TEAM

Securing the team is an extension of securing the production.

Security training of all employees to raise awareness of both the security best practices and the security risks which apply to each personally in addition to physical and digital assets.

Include security awareness in production and safety meetings. Highlight physical perimeters, safe areas and methods to report security failures, risks and concerns.

An individual compromised physically (robbed) or virtually (hacked, phished) may not only be personally harmed but the harm may extend to the production if they are robbed of production assets or they infect production systems with viruses or malware or if their identity is spoofed for systems access.

4.7 DIGITAL ASSETS

4.7.1 DIGITAL ASSET MANAGEMENT (DAM) POLICY

Digital assets must be tracked, stored and managed the same as physical assets. Assigning the responsibility to an individual or individuals across departments is recommended.

4.7.2 DIGITAL ASSET COPIES

A single copy of digital assets should exist (Backup and archive copies excepted.) Fewer copies mean fewer assets to protect. Local shared storage and cloud services which provide links to files rather than copies of the files reduce the potential number of digital asset copies and make managing and tracking access to them simpler.

4.8 COMPANY COMMUNICATIONS

4.8.1 E-CORRESPONDENCE

Communications (paper correspondence, emails, texts, chats) drafted by production staff are production work product and subject to the protections of the non-disclosure agreements and asset security policies. It is natural for paper correspondence to be filed and stored in production paper files. The same should apply to electronic communications – e-correspondence should be stored in production data storage e.g. production email server, production shared file system.

There can be no assumption of confidentiality, privacy or security when personal communications services (e.g. Gmail) are used. Additionally, when personal communications services are used the individual is in possession of those work product communications which are the property of production.

Attachments vs File Links:

- Sending a link to a file leaves the file securely stored within the production's control. All access to the link is logged. The access permissions appropriate to the recipient may be set and may be altered as needed.

- If email and email attachment encryption are available, enforcing their use is recommended. Equally for encrypted messaging.
- Files sent as unencrypted attachments create additional copies of data assets which are outside the control of production. Once received, the recipient may share the unencrypted attachments and the number of copies ensuing are unknown and untraceable to production.

4.9 SECURE ASSET & DATA DESTRUCTION

4.9.3 FINISHED ELEMENTS

Finished elements (e.g., script sides, rejected designs, works-in-progress once final version is elected, tests, temp versions, check discs, test prints, mock-ups, ADR scripts) should be destroyed at the earliest opportunity after the usefulness has expired.

Establish a clear chain of approval for determining the retention and destruction of 'finished elements'. Some ‘elements’ may have marketing value for the “making of” or “bloopers” etc. and should be retained after their usefulness to the production is finished but, rejected designs, early works-in-progress, unflattering reference images etc. should be protected against leaks as much as the 'hero' versions - they can cause far more damage to the image and marketing of the content.

(RETURN TO TABLE OF CONTENTS)

V. VIRTUAL – DATA – SECURITY

5.1 WIDE AREA NETWORK (WAN) AND INTEROFFICE CONNECTIONS

5.1.1 NETWORK DIAGRAMS

IT manager or contractor should draw the diagram of the intended network and explain it to the production manager or designated security team prior to installing. The diagram should highlight the purpose and relationship of each component plus where and how the network may be accessed by authorized and unauthorized personnel. The production manager is responsible for allocating funds and personnel, their understanding of the requirements will better enable them to do so

appropriately. This will enable proper security to be implemented around the network components and understanding of the potential weaknesses and mitigation steps to be taken.

5.2 FIREWALL AND SECURITY SERVICES

5.2.1 FIREWALL GUIDELINES

At a minimum, all computers accessing shared information, including restricted access to content, must have a firewall installed, as well as anti-virus/malware software.

5.2.4 EMAIL FILTERING

Do not assume email filtering (anti-virus, anti-malware, etc.) will catch ALL phishing emails, infected attachments or dangerous domains. There are new threats created daily. Employees should be regularly reminded to watch out for suspicious emails and, trained to recognize them.

Employee training to spot suspicious emails is essential. Each employee is your first and last line of defense.

5.2.5 WEB FILTERING

Clear and enforced policies should be established prohibiting the use of unauthorized file sharing sites and sites known for malware, viruses and other malicious activity.

5.3 PRODUCTION NETWORKS

5.3.1 PRODUCTION NETWORK RESTRICTIONS

Office networks should be set up to separate information and digital content to protect against inappropriate or unauthorized access and to limit damages in the case one network is compromised.

Do not post Wi-Fi passwords publicly. They should be provided to authorized users only and kept at all times confidential.

Set up a Guest Wi-Fi network for visitors to allow them access to the internet but no access to production networks.

5.5 SHARED STORAGE, SAN AND NAS SERVERS

5.5.2 SEGREGATION OF STORAGE

Shared storage should be segregated just as physical spaces and production networks. Segregation means to limit the data stored and the persons and devices accessing that data into small segments or groups such as separate servers and limited privileged access folders. (See section *5.10 Privileged Access Management & User Accounts* and the *"Least Privilege Principle" definition*.)

Shared storage is a frequent means for hackers to penetrate and infect or steal corporate data. Segregated storage can limit the amount of content and data affected by a breach.

5.6 ELECTRONIC FILE TRANSFER AND DATA I/O NETWORK

5.6.4 TRANSFER TOOLS & SERVICES

Transfers of content should only occur over secure, encrypted file-transfer platforms.

Do not use any free or consumer grade transfer services.

5.8 USE OF CLOUD SERVICES

5.8.1 SELECTION OF CLOUD SERVICES – SECURITY VETTING

Prior to using a Cloud Service, vet their security practices, breach history and responses.

Do not rely on marketing materials to vet a cloud providers security, many focus entirely on their service solution and do not seriously address security until after a breach. We hear about major breaches such as Salesforce and Yahoo but there are small breaches every day.

Note: where third party facilities rely on cloud services, the same vetting should occur.

5.9 DEVICE SECURITY

5.9.1 SECURING COMPUTER AND MOBILE DEVICES

Productions should issue computers enrolled in an endpoint management or mobile device management system to individuals creating, editing, receiving, sending, storing and/or managing content and its metadata (e.g. individuals creating, editing, storing and/or managing media, designs, production information, accounting and payroll records.)

If unable to issue computers and production allows individuals to use their own computers (also known as 'bring your own devices' BYODs), the production should require all BYOD devices to be enrolled in a company managed endpoint management or mobile device management system.

5.9.6 SECURITY FOR DEVICES ACCESSING THE INTERNET

Internet access is essential to business functions but simultaneously exposes businesses to uncountable external threats. The production's access to the internet is its most exposed Perimeter Access Point. Digital versions of all the security measures (and more) needed to protect our physical perimeter are needed to protect our digital perimeter.

Make sure when setting up the production's office networks and on-premise servers that appropriate security measures are installed. Consumer grade solutions do not provide the security layers necessary to safe guard a production's data and content.

Every individual who connects with the internet and connects with the company's data (e.g. using their personal device to access both their personal services (email, shopping, Facebook, etc.) and to access the company's data (shared file storage) creates a bridge between the public internet and the company's data and content. A crew member who clicks on a phishing email on their personal device can then infect the company's services when they connect or upload files to the company's file storage (e.g. opening a phishing text message on their mobile device and then uploading images (e.g. continuity stills) from that same device to the company's image bank.)

Productions should consider the data and content access granted to individuals and the devices (desktops, laptops, tablets and smartphones) those individuals use for that access. Every device which accesses the public internet, personal services and accounts that are not monitored and secured by the production, create unprotected openings in the production’s digital perimeter.

5.9.7 DEVICE FIREWALLS

All computers used for production purposes should have a firewall installed and active.

5.9.8 DEVICE ENCRYPTION

All computers and mobile devices that receive, send, manipulate, or store content should be encrypted with whole disk encryption. For desktops and laptops, Windows Bitlocker and Apple FileVault 2 are preferred.

Encryption adds password or PIN authentication to access data stored on the devices.

5.10 PRIVILEGED ACCESS MANAGEMENT & USER ACCOUNTS

5.10.1 CENTRAL ADMINISTRATION SYSTEM/DIRECTORY SERVICES

An identity manager directory service should be used to manage user activation, deactivation and access authentication to any infrastructure, shared storage, server, cloud services, or workstation computer or laptop device.

Access to all systems (servers, computers, applications, cloud services) which contain production information and content must require authenticated access: unique user identity and access key (e.g. username and password).

Systems which contain more sensitive data and content should require multi-factor authentication (e.g. a text message to a mobile device, a USB dongle)

5.10.3 ACCESS RIGHTS ADMINISTRATION

"Least Privilege" is the concept whereby individuals or groups are only granted access to the minimum areas, information, resources, and controls necessary to fulfill their job role. As examples:

- General set crew do not need access to editing rooms: access to the editing rooms should be limited to editors and key creatives invited to review content with the editors.
- Accounting staff do not need to access the Concept Artists design folders and files, the Concept Artists don't need access to any Accounting folders or files to accomplish their jobs.

Access to shared folders on a server or cloud sharing service should be limited both in access and the privileges of that access (read, edit, print, download etc.)

Assigning access rights to User Groups rather than individual users greatly simplifies rights management. Each User Group is defined by the resources, data and access permissions the group requires. These settings must be carefully established. Assigning users to the appropriate group or changing their group assignment if their role changes is a simple process.

5.10.4 TRUSTED DEVICE ACCESS MANAGEMENT

All devices, including personal computers and mobile devices, which need to access production networks need to be trusted. In order to become a trusted device, a device needs to be compliant with the device security policies and be monitored by production security administration and their security monitoring endpoint or mobile device managers. Users should be trained to understand the benefits of device registration and endpoint management which will protect them in the case of loss or theft of their devices.

5.10.5 PASSWORD POLICY

Policies should be established to enforce the use of unique accounts and strong passwords for all information systems.

Sharing of passwords should be prohibited (including between executive and assistant.)

Passwords should have a minimum length of eight characters for any account, 12 or more characters is preferred.

Good password policy is valuable to everyone at work and at home. Training your production staff is time well spent for all.

5.11 PATCH / UPDATE MANAGEMENT

5.11.1 PATCH MANAGEMENT

Malware, viruses and attack vectors are invented every day and the manufacturers and developers of devices and device operating systems and applications need to issue patches to address the newly exposed vulnerabilities. Keeping systems up to date with the most current security patches is essential.

Whereas updates used to primarily address functionality and would often cause havoc for users, today updates primarily provide security patches to correct for newly discovered vulnerabilities. Many of the successful cyber-attacks have relied on older operating systems and unpatched machines.

5.12 DATA BACKUP AND RECOVERY

5.12.2 DATA BACKUP

All computers used for production purposes should be set up for regular backups.

5.13 VULNERABILITY ASSESSMENT AND PENETRATION TESTING

5.13.1 PENETRATION TESTING

Network penetration tests should be conducted after initial network setup and significant operational changes have been performed (e.g. hardware or software updates) on the firewall.

Do not assume the trustworthiness, nor the security expertise of third party IT services providers. Check references, particularly from IT security professionals. Check credentials, ask for security certifications. Check if vendor has done background checks of their staff. If available, use a Studio approved IT vendor.

Do not assume that even the most trustworthy IT professional is immune to errors.

The systems setup should be tested by a different provider and critical security issues should be remediated in accordance with the Production's Security Policy.

(RETURN TO TABLE OF CONTENTS)

VI. PLANNING & RESPONSE TO SECURITY BREACHES

6.1 PLANNING MANAGEMENT AND WORKFLOWS

6.1.1 SECURITY RISK ASSESSMENTS

Risk assessments should be conducted at commencement of pre-production, prior to principal photography and editorial, and periodically reviewed upon changes to any content workflows, to identify critical resources and dependencies and assess the risks related to each stage of asset workflows.

We do Safety Risk Assessments for every filming location, major stunt or special effects filming. We need to do the same for securing our production assets.

6.1.2 BUSINESS CONTINUITY MANAGEMENT (BACKUP PLANNING)

Productions should prepare a Business Continuity Plan which addresses each stage of the production workflow and each location where production activities will occur.

A business continuity plan outlines the steps and procedures that should be taken in the event that a disruption to standard operations occurs in order to limit damages caused by the disruption. Examples of disruptions are loss of power, loss of internet, equipment failure, employee termination, intruders, discovery of a security breach, loss of data, data theft etc.

6.3 RESPONDING TO BREACHES

6.3.1 ANONYMOUS REPORTING

Anonymous reporting should be made available to production crew and contractors for reporting of content protection and piracy concerns.

6.3.2 INCIDENT RESPONSE

A plan for who should be notified - when and by whom - should be included in the security policies. In cases of content leaks, the studio has teams available to respond quickly, investigate and mitigate damages.

As of 12/1/2018: The law enforcement office in Los Angeles to contact is the Office of the District Attorney - Deputy D.A. Warren Kato: wkato@da.lacounty.gov; 213-257-2440

(RETURN TO TABLE OF CONTENTS)

CDSA's Production Security Working Group (PSWG) is open to participation by CDSA Board member companies and other invited guests. For questions, comments, or to communicate with the PSWG's Co-Chairs, please e-mail: pswg@CDSAonline.org

ABOUT CDSA

The Content Delivery and Security Association (CDSA) is the worldwide advocate and forum for the secure and responsible production, distribution and storage of media & entertainment content. CDSA is a partner with the Motion Picture Association of American (MPAA) in the Trusted Partner Network (TPN), which helps prevent leaks, breaches and hacks of movies and television shows through a shared software platform and a single, industry-supported set of Best Practices. Originally Founded in 1970 as the International Tape Association (ITA), this 501(c)6 non-profit issued its first content security assessment standards in 1999. CDSA's leadership includes senior security executives from over 25 international media & entertainment companies.

For additional information, visit www.CDSAonline.org