CDSA
Content Delivery & Security Association

Film & TV Production Security Guidelines

Developed and Maintained by CDSA's
Production Security Working Group

www.CDSAonline.org

Table of Contents

Table of Contents 1

INTRODUCTION 5

AUTHORS 6

PURPOSE 6

TARGET AUDIENCE 6

ORGANIZATION 7

THE SECURITY LAYERS 7

APPENDICES: SUMMARIES & REFERENCES 8

KEY TO GUIDELINE FLAGS 8

PERSONS RESPONSIBLE 8

I. DEFINITIONS 9

II. PEOPLE 15

2.1 INDIVIDUAL RESPONSIBILITY 16

2.1.1 SECURITY MANAGEMENT TEAM 16

2.1.2 ALL CREW AND CONTRACTORS 17

2.2 ENGAGING EMPLOYEES & CONTRACTORS 18

2.2.1 BACKGROUND CHECKS, REFERENCES & CERTIFICATIONS 18

Background Checks & References 18

Third Party Certifications & Warranties 19

2.2.2 CONFIDENTIALITY 19

Non-Disclosure Agreements 20

Social Media Awareness 20

2.2.3 SECURITY REQUIREMENTS 20

2.2.4 SECURITY AWARENESS TRAINING 21

2.2.5 DAILY HIRES AND EXTRAS MANAGEMENT .. 22

2.2.6 EXIT PROCESS UPON COMPLETION OF SERVICES OR TERMINATION 22

2.3 ACCESS CONTROLS 23

2.3.1 IDENTIFICATION 23

Enforcement of Identification Cards Use 23

Temporary & Visitor IDs 23

2.3.2 SEGREGATION OF ACCESS AND DUTIES 24

Duties 24

Access 24

2.3.3 CONTRACTORS AND THIRD-PARTY PERSONNEL ACCESS 25

On Premises (Offices, Locations, Stages) 25

Off Premises (Third Parties) 25

2.3.4 TEMPORARY (DAILY) PERSONNEL ACCESS .. 26

2.3.5 VISITOR SUPERVISION 26

2.3.6 COURIERS AND SHIPPERS 26

III. PHYSICAL – BRICK & MORTAR – SECURITY .. 28

3.1 FACILITY SECURITY 29

3.1.1 IDENTIFY PERIMETERS 29

3.1.2 PERIMETER 29

3.1.3 SHARED FACILITIES – RENTAL SPACES 30

3.1.4 SHARED FACILITIES – VENDORS 31

3.2 PHYSICAL SECURITY & SECURITY GUARDS 31

3.2.1 GUARD ASSIGNMENTS & AWARENESS 31

3.2.2 GUARD PATROL PROCEDURES 31

3.2.3 GUARD AUTHORITY 32

3.2.4 GUARD KEYS AND ACCESS CODES 32

3.3 FACILITY AUTHORIZED ACCESS 33

3.3.1 AUTHORIZED ACCESS CONTROL PROCEDURES 33

3.3.2 PHYSICAL ACCESS CONTROLS 33

3.3.3 ACCESS POINTS OF ENTRY – CHECK-IN/CHECK-OUT 34

3.3.4 PHYSICAL ACCESS LOGGING 34

3.3.5 VISITOR ACCESS LOGS 35

3.3.6 TEMPORARY HIRE ACCESS LOGS 35

3.3.7 ELECTRONIC ACCESS (KEY-LESS) 35

3.3.8 PHYSICAL KEY MANAGEMENT 36

3.3.9 LOCK MAINTENANCE 37

3.3.10 USE OF PORTABLE DIGITAL DEVICES WITHIN RESTRICTED AREAS 37

3.4 LOCKED STORAGE AND SAFES 38

3.4.1 LOCK-UPS, VAULTS AND SAFES....................38

3.4.2 SAFE SPECIFICATIONS..................................39

IV. ASSET MANAGEMENT 40

4.1 PSEUDONYMIZED SECURITY TITLE.......................41

4.1.1 USE OF ALIAS TEMPORARY TITLES...............41

4.2 HIGH VALUE/CONFIDENTIAL SECURITY DESIGNATION 41

4.2.1 ASSET SECURITY DESIGNATION 41

4.3 INVENTORY POLICIES 42

4.3.1 RECORDING CHAIN OF CUSTODY 42

4.3.2 INVENTORY MAINTENANCE.........................43

4.3.3 INVENTORY PIPELINE & LOG ACCESS 43

4.4 ASSET TRACKING..44

4.4.1 LOGGING & TRACKING 44

4.4.2 DIGITAL ASSETS ON PORTABLE OR LOCAL DEVICES (THEIR PHYSICAL FORM)........................44

4.5 PEOPLE ARE ASSETS 45

4.5.1 SECURITY FOR THE TEAM............................45

4.6 PHYSICAL ASSETS – SECURING, STORAGE, SHIPPING 46

4.6.1 SHIPPING AND RECEIVING POLICIES...........46

4.6.2 SHIPPING PACKAGING 46

4.6.3 SHIPPING PACKAGE LABELING.....................46

4.6.4 STAGING AREA MONITORING......................47

4.6.5 DAMAGES, LOSSES & DISCREPANCIES OF SHIPPED ASSETS..47

4.6.6 COURIER AND SHIPPING RECEIPTS/LOGS ...48

4.6.7 CLOSED OFFICE HOURS / OVERNIGHT DELIVERIES 48

4.6.8 PORTABLE AND LOCAL DEVICES & COMPUTERS...48

4.6.9 INVENTORY COUNT PROCEDURE 49

4.7 DIGITAL ASSETS..50

4.7.1 DIGITAL ASSET MANAGEMENT (DAM) POLICY 50

4.7.2 DIGITAL ASSET COPIES.................................51

4.8 COMPANY COMMUNICATIONS 51

4.8.1 E-CORRESPONDENCE 51

Email 51

Instant Messaging 52

4.8.2 COMMUNICATION DISTRIBUTION LISTS..... 52

4.9 SECURE ASSET & DATA DESTRUCTION 53

4.9.1 DAMAGED STOCK CONTAINING CONTENT 53

4.9.2 DESTRUCTION OF CONTENT........................ 53

4.9.3 FINISHED ELEMENTS 54

4.9.4 STAGING FOR RECYCLING & DESTRUCTION54

4.9.5 THIRD PARTY DESTRUCTION OF CONTENT. 55

4.9.6 DESTRUCTION OF ASSETS LOGGING 55

V. VIRTUAL – DATA – SECURITY........................56

5.1 LOCAL AREA NETWORK (LAN), WIDE AREA NETWORK (WAN) AND INTEROFFICE CONNECTIONS 57

5.1.1 NETWORK DIAGRAMS................................. 57

5.1.2 POINT-TO-POINT CONNECTIONS (DATA TRANSFER CHANNELS) 57

5.2 FIREWALL AND SECURITY SERVICES 58

5.2.1 FIREWALL GUIDELINES................................ 58

5.2.2 FIREWALL MANAGEMENT 58

5.2.3 SEGREGATION 59

5.2.4 EMAIL FILTERING... 59

5.2.5 WEB FILTERING 60

5.2.6 DNS POLICIES... 60

5.2.7 LAN SECURITY.. 61

5.2.8 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP).. 61

5.3 PRODUCTION NETWORKS.................................. 62

5.3.1 PRODUCTION NETWORK RESTRICTIONS 62

5.3.2 INTERNET ACCESS RESTRICTIONS 63

5.3.3 CONTENT TRANSFER NETWORK 64

5.3.4 DATA I/O (INBOUND/OUTBOUND) ACCESS 64

5.3.5 SWITCHING.. 65

5.3.6 DUAL-HOMING / BRIDGING SEGREGATED NETWORKS 65

5.4 WIRELESS NETWORKS.. 65

5.4.1 WIRELESS NETWORKS GENERAL..................65
5.4.2 PRODUCTION WIRELESS NETWORKS 66
5.4.3 PRE-SHARED KEY (PSK) USAGE AND AUTHENTICATION IN PRODUCTION WI-FI NETWORKS..67
5.5 SHARED STORAGE, SAN AND NAS SERVERS 67
5.5.1 LOCAL DATA STORAGE - SAN / NAS SECURITY 67
5.5.2 SEGREGATION OF STORAGE 68
5.6 ELECTRONIC FILE TRANSFER AND DATA I/O NETWORK..68
5.6.1 CONTENT TRANSFER POLICIES & PROCEDURES...68
5.6.2 CONTENT TRANSFER SYSTEM GUIDELINES .69
5.6.3 CONTENT TRANSFER / DATA IO SYSTEMS...70
5.6.4 TRANSFER TOOLS & SERVICES 70
5.6.5 WEB PORTAL SYSTEMS................................70
5.6.6 PORTAL / TRANSFER SYSTEM USERS 71
5.6.7 CONTENT ENCRYPTION KEY 71
5.6.8 DATA INGEST ANTI-VIRUS/ANTI-MALWARE/MALICIOUS BEHAVIOUR SCANNING..71
5.6.9 SECURE DELETION FROM DATA I/O SYSTEM 71
5.7 REMOTE ACCESS TO PRODUCTION NETWORKS...72
5.7.1 REMOTE ACCESS POLICY 72
Remote Access Settings Policy............................ 72
Remote Access User Policy 72
5.7.2 REMOTE ACCESS – USER AUTHENTICATION 73
5.7.3 SITE-TO-SITE CONNECTIONS........................73
5.7.4 REMOTE SYSTEM ADMINISTRATOR / IT SUPPORT ACCESS...73
5.7.5 THIRD-PARTY REMOTE ACCESS...................74
5.8 USE OF CLOUD SERVICES....................................74
5.8.1 SELECTION OF CLOUD SERVICES – SECURITY VETTING..74
5.8.2 CLOUD ACCESS SECURITY BROKERS 75
5.8.3 CLOUD SERVICES SETTINGS 75
5.8.4 CLOUD STORAGE / FILE SHARING SERVICES76
5.9 DEVICE SECURITY 77
5.9.1 SECURING COMPUTER AND MOBILE DEVICES 77
Company provided devices 77
Managed employee owned devices: Bring Your Own “BYOD”s 78
Unsupervised BYODs (NOT RECOMMENDED)..... 79
5.9.2 COMPUTERS STORING CONTENT/CONFIDENTIAL DATA 79
5.9.3 I/O DEVICES AND DATA TRANSFER PORTS (E.G. USB PORTS) 79
5.9.4 WORKSTATION/DEVICE GUEST ACCOUNTS 80
5.9.5 INTERNET ACCESS LIMITATIONS 80
5.9.6 SECURITY FOR DEVICES ACCESSING THE INTERNET 80
5.9.7 DEVICE FIREWALLS...................................... 81
5.9.8 DEVICE ENCRYPTION................................... 82
5.9.9 SERVER HARDENING 82
5.9.10 IOT AND NETWORK DEVICES (PRINTERS, MULTI-PURPOSE, REMOTE MONITORING, ETC.). 82
5.10 PRIVILEGED ACCESS MANAGEMENT & USER ACCOUNTS 83
5.10.1 CENTRAL ADMINISTRATION SYSTEM/DIRECTORY SERVICES 83
5.10.2 ACCOUNT MANAGEMENT PROCESS......... 83
5.10.3 ACCESS RIGHTS ADMINISTRATION 84
5.10.4 TRUSTED DEVICE ACCESS MANAGEMENT 85
5.10.5 PASSWORD POLICY 85
5.10.6 MULTI-FACTOR AUTHENTICATION POLICY 87
5.10.7 ACCESS RIGHTS ASSIGNMENTS 87
5.10.8 ACCESS TO DATA ON PORTABLE AND LOCAL DEVICES/COMPUTERS.. 88
5.11 PATCH / UPDATE MANAGEMENT 88
5.11.1 PATCH MANAGEMENT 88
5.11.2 CHANGE MANAGEMENT 89
5.12 DATA BACKUP AND RECOVERY......................... 90
5.12.1 DATA BACKUP STRATEGY 90
5.12.2 DATA BACKUP 90
5.12.3 BACK UP COPIES.. 91
5.12.4 BACK UP OF PERSONAL DEVICES 91

5.13 VULNERABILITY ASSESSMENT AND PENETRATION TESTING 92

5.13.1 PENETRATION TESTING 92

5.13.2 TESTING POLICY 92

5.13.3 VULNERABILITY SCANS 93

5.14 SYSTEMS AND SECURITY MONITORING & LOGGING 93

5.14.1 SYSTEM LOGGING 93

5.14.2 MONITORING CONTROLS SETTINGS 94

5.14.3 AUTOMATIC NOTIFICATIONS 94

VI. PLANNING FOR SECURITY & RESPONSE TO BREACHES 96

6.1 PLANNING MANAGEMENT AND WORKFLOWS ...97

6.1.1 SECURITY RISK ASSESSMENTS 97

6.1.2 BUSINESS CONTINUITY MANAGEMENT (BACKUP PLANNING) 98

6.1.3 INCIDENT REVIEW 98

6.2 LOG REVIEWS 99

6.2.1 ACCESS LOGS 99

6.3 RESPONDING TO BREACHES 100

6.3.1 ANONYMOUS REPORTING 100

6.3.2 INCIDENT RESPONSE 100

(RETURN TO TABLE OF CONTENTS)

INTRODUCTION

AUTHORS

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

TARGET AUDIENCE

The guidelines are dense and it is not expected that all producers and crew will read them cover to cover. They should serve as a **reference resource for all** to go to when addressing specific policies, procedures or implementations.

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.

ORGANIZATION

THE SECURITY LAYERS

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, 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

The assets 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.

APPENDICES: SUMMARIES & REFERENCES

The appendices are intended as useful handouts for those who may not read the full guidelines. We have included:

- The One-Page Security Checklist
- General Guidance Summary
- Individual Responsibility
- Helpful reference website list

KEY TO GUIDELINE FLAGS

PERSONS RESPONSIBLE

Executive Management:	"**EXEC MGMT**"	those who must understand, establish and mandate policies
Department Heads:	"**ALL KEYS**"	those who should advise and guide their departments
	"**PROD MGMT**"	those who oversee the general implementation, staffing and budgeting of policies
	"**LOC MGMT**"	those who source and manage production facilities and locations
Security Team	"**SEC TEAM**"	those assigned security oversight
IT Managers	"**IT**"	those responsible for the IT management, setup, monitoring, and maintenance (staff or 3rd parties)
Contractors	"**3RD**"	third party engagement recommended

EXEC MGMT	**DEPT HD**	**SEC TEAM**	**IT**	**3RD**

Search the document using the terms above to go directly to role appropriate topics or see headings in the Table of Contents.

(RETURN TO TABLE OF CONTENTS)

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 only, examples being:

- Documents – scripts, sides, treatments, call sheets, 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 Filemaker, Avid, Shotgun, Stornext etc.
- Electronic communications - emails

Physical Asset, an asset 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.
- People – the cast and crew who the production are dependent on

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 directly 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 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 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.

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 in order 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 WI-FI.
- *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.
- *WI-FI 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

EXEC MGMT **ALL KEYS** **SEC TEAM**

Best Practice

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.

Responsibilities for this Security Management Team include, but are not limited to:

- Creating information security management policies and processes
- Spreading awareness of security policies and processes to the production employees and contractors
- Providing methods and points of contact for production employees and contractors to report security concerns or breaches
- Auditing content workflows to identify key control points and areas of vulnerability
- Measuring policy and control effectiveness
- Detecting and correcting risks
- Proactively monitoring information systems and physical security to identify and respond to suspicious activity
- Monitoring and reporting inappropriate and / or suspicious activity
- Providing input and feedback toward the development and maintenance of the Business Continuity Plan

Alternative Approach

Each department should have at least one person tasked and trained on security policy, procedure and implementation applicable to their department's workflows.

There should be a clear channel for reporting any security vulnerabilities, suspicions and breaches including a means for anonymous reporting.

Security policy training for all production employees and contractors emphasizing every person's responsibility in the overall security of the production.

Implementation Tip and/or Reasoning

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 Safety 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

EXEC MGMT	**ALL KEYS**	**SEC TEAM**	**IT**	**3RD**

Best Practice

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.
    - If you receive instructions to take an action that may put assets at risk via email or chat, call the person to verify the instructions.
    - Reporting spam, phishing or any suspicious communications.
- ***When uncertain about any policy or best practice, asking for guidance***.

Implementation Tip and/or Reasoning

Ask for guidance, ask for training, use common sense and be conscientious, help others to do the same. Don't be the one who left the door open.

2.2 ENGAGING EMPLOYEES & CONTRACTORS

2.2.1 BACKGROUND CHECKS, REFERENCES & CERTIFICATIONS

EXEC MGMT **PROD MGMT**

Best Practice

Background Checks & References

Prior to the first day of engagement, background checks should be conducted for all employees and/or third-party personnel who have access to assets where permitted and applicable by local law. Guidelines for background checks include, but are not limited to:

- Identity should be verified with a valid proof of identification (e.g. driver's license or identity card)
- Methods used should be proportional to sensitivity of assets and risks of assets theft or leakage
- Academic, and professional qualification checks should be conducted where permitted and applicable
- Employment and personal references should be checked, and
- When background checks are not allowed by local law, use *Alternative Approach*.

Third Party Certifications & Warranties

Third-party vendors providing personnel services (e.g. extras casting services, visual effects companies, picture and sound companies, fabricators etc.) should provide contractual warranties that security training and policies meeting the production company's requirements and/or the MPAA's Best Practices are implemented.

Third-party vendors should provide a list of the names of all personnel assigned to the project to the production in order for their personnel to be verified upon entry/access to the production facilities and/or assets.

Alternative Approach

Prior to the first day of engagement, reference checks should be conducted for all employees and/or third-party personnel who have access to assets. References should include, but are not limited to:

- Professional qualification checks should be conducted where permitted and applicable
- Employer references should be checked.

Implementation Tip and/or Reasoning

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

EXEC MGMT **PROD MGMT**

Best Practice

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.

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.

Implementation Tip and/or Reasoning

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

Do not assume employees and third parties understand the non-disclosure/confidentiality agreement: explain it in basic practical terms.

Employment and third-party non-disclosure agreements should explicitly describe activities which are forbidden.

2.2.3 SECURITY REQUIREMENTS

EXEC MGMT **PROD MGMT**

Best Practice

Security requirements should be included in all employee and third-party contracts, including language stating that disciplinary action may be taken if security requirements are not followed.

Alternative Approach

Security requirements should be included in all employees and third-party contracts. At a minimum, reference responsibility to learn and adhere to production security guidelines.

Implementation Tip and/or Reasoning

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

EXEC MGMT **PROD MGMT**

Best Practice

All Employees and on-production third-party personnel who have access to assets should be given security awareness training upon hiring, before being granted access to assets, upon changes in security protocols, and if engagement exceeds a year, at least annually thereafter. Training topics should cover the best practices provided by these guidelines which are pertinent to the individual's job role.

Procedures should be implemented to track and document completion of the security awareness training.

Alternative Approach

Require all Employees and on-production third-party personnel who have access to assets, to read the Production Individual Security Responsibilities Guidelines prior to commencing work or accessing assets and to sign an affidavit confirming to have read and understood the guidelines.

Implementation Tip and/or Reasoning

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.

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

EXEC MGMT **PROD MGMT**

Best Practice

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.

Implementation Tip and/or Reasoning

Based on their role, the necessary background checks and training will be extremely limited. However, requiring confidentiality agreements and providing social media and security awareness training or instructions is essential. Daily personnel are frequently ignored while often given extensive access. They are harder to keep track of while engaged and following their completion of engagement. And, they have much less, if any, loyalty committed to the production.

2.2.6 EXIT PROCESS UPON COMPLETION OF SERVICES OR TERMINATION

EXEC MGMT **ALL KEYS** **SEC TEAM** **IT** **3RD**

Best Practice

Exit process upon termination of employment or contract should be documented. This includes, but is not limited to:

- Documenting and storing history of terminated personnel in production payroll files
- Documenting reasons for termination in the record (e.g., theft, content or sensitive information breach, other policy breach)
- Requiring departing personnel to immediately return and/or securely delete all assets in their possession
- Formally reminding departing personnel of their ongoing confidentiality and non-disclosure responsibilities
- Requiring company photo IDs to be returned immediately upon termination
- Revoking physical access rights (i.e., keys and badges) and digital access rights (applications, cloud services, networks and data files) immediately upon termination.

Implementation Tip and/or Reasoning

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

PROD MGMT	SEC TEAM	IT

Best Practice

Production IDs should not reference the company or address by name nor provide information to lead unauthorized persons to production spaces or facilities.

They should include a contact for reporting found IDs.

They should include a photograph of the bearer.

They should have design differences to easily identify the role of the bearer and what access privileges they have been granted (e.g. red border for visitors with restricted accompanied access, green border for persons with ALL access, a camera icon for persons permitted to photograph...)

Enforcement of Identification Cards Use

Proper use of photo IDs should be enforced for production crew and contractors. Enforcement guidelines include, but are not limited to:

- Security guards, assistant directors, office receptionists and other designated employees (e.g. location dept staff or set production assistants) should check all production crew and contractors upon entry to production spaces.
- Production crew and contractors should be required to report a lost or stolen photo ID immediately
- A process for immediately revoking photo IDs upon termination should be in place
- Employees should be encouraged to challenge a person without proper visible identification

Temporary & Visitor IDs

Temporary/Visitor IDs should be provided to all visitors and short-term employees including daily cast, crew and extras.

- Security guards, assistant directors, office receptionists and other designated employees should be kept informed of the number and location of temporary badge holders
- Temporary IDs should be easily identifiable with a specific area and/or duration of validity
- Verify visitor and short-term employee identities prior to logging and issuing them temporary/visitor IDs.

Alternative Approach

Employees may report individuals without ID to Security or Management in lieu of confronting the individual directly.

Implementation Tip and/or Reasoning

Tools - software and printers are becoming readily available, many have smartphone apps for quick photo capture.

Consider where and in what circumstances the IDs will be worn and design them to avoid loss or interference with equipment. In the case of on-camera cast and extras plan for a means to hide them or store them.

If electronic keycards are used as ID cards, temporary ID holders should be issued non-keycard ID badges.

No unidentified persons should be issued production IDs.

2.3.2 SEGREGATION OF ACCESS AND DUTIES

PROD MGMT SEC TEAM IT

Best Practice

Duties

To protect against any one individual's having unilateral control of assets, duties should be segregated to eliminate overlap of job functions within the workflow where possible. Examples of distinct job functions fulfilled by different personnel:

- Vault and server management
- Shipping order creation and validation
- Shipping and receiving
- Physical assets movement (clerks and runners)
- Digital assets transfer (inbound and outbound) management
- Digital assets management and IT administration
- Digital assets creation, duplication and destruction
- Individuals responsible for assigning access to systems and end users of those systems
- Encryption key issuance and creation of encrypted content with the key

Access

Personnel who require access to assets and content should be assigned to Job Roles and User Groups based on their department and their duties within the departments:

- Job roles which require the receipt of production information and notifications only (e.g. set technical crew.)
- Job roles which review, comment, annotate the creative process.
- Job roles which create and manipulate digital assets (e.g. editors, designers, accountants, certain production staff.)

- Job roles which are entitled to share information and content (e.g. producers, production management, department heads, specified asset managers such as assistant editors, etc.)
- Job roles which are entitled to administer specific resources (e.g. cloud applications)
- System and Network Administrators

Physical access to restricted areas should be limited to personnel with the appropriate relevant job roles. See paragraph *2.3.1 Identification* regarding badge designs for easy role and access identification.

For digital asset access, see section *5.10 Privileged Access Management and User Accounts*.

Alternative Approach

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

Implementation Tip and/or Reasoning

Limit single person direct and unilateral control of assets.

Wherever possible, create a 2nd check for assets status, location and movement by a separate individual

Map out workflow, separate employee duties to single steps of the workflow with confirmed hand-offs to next step and employee of the workflow

2.3.3 CONTRACTORS AND THIRD-PARTY PERSONNEL ACCESS

PROD MGMT **SEC TEAM**

Best Practice

On Premises (Offices, Locations, Stages)

Policies and procedures should be maintained to monitor access of contractors and third-party personnel. Guidelines include but are not limited to:

- require adherence to the company security policies and procedures
- grant minimum necessary access to premises and/or assets
- provide ID badges
- do not grant access to work premises unaccompanied or unsupervised

Off Premises (Third Parties)

Verify the third-party off-site security policies and implementation meet the production's security requirements.

Facilities that handle assets out of the control of the producer should adhere to the MPAA's best practices and have a current TPN, MPAA or Studio security appraisal. These best practices require strict personnel management and third-party personnel supervision.

Implementation Tip and/or Reasoning

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.)

2.3.4 TEMPORARY (DAILY) PERSONNEL ACCESS

ALL KEYS SEC TEAM

Best Practice

Temporary staff (e.g. Daily Hires) should be supervised by a production full-time employee at all times.

Alternative Approach

At a minimum, temporary staff should be accompanied whenever accessing restricted areas.

Implementation Tip and/or Reasoning

Dailies should not work alone in restricted areas.

2.3.5 VISITOR SUPERVISION

ALL KEYS SEC TEAM

Best Practice

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.

Implementation Tip and/or Reasoning

Do not allow visitors on days when the production will be unable to provide proper supervision. Require hosts of visitors to acknowledge their responsibility for the visitors.

2.3.6 COURIERS AND SHIPPERS

PROD MGMT SEC TEAM

Best Practice

Couriers and shippers should have clearly defined pick-up and drop-off locations which are monitored or attended at all times.

If the pick-up or drop-off point is within the production perimeter:

They should be treated as visitors, registered and provided temporary ID badges.
They should be escorted at all times to, at and from the pick-up or drop-off location.

Implementation Tip and/or Reasoning

Establish pick-up and drop-off points that are secure and easy to monitor but which require minimum access to couriers and shippers.

(RETURN TO TABLE OF CONTENTS)

III. PHYSICAL – BRICK & MORTAR – SECURITY

3.1 FACILITY SECURITY

3.1.1 IDENTIFY PERIMETERS

	LOC MGMT	SEC TEAM

Best Practice

Identify all points of access between public spaces and production-controlled spaces. Identify internal perimeters between areas of restricted access and areas open to all visitors.

Implementation Tip and/or Reasoning

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

EXEC MGMT	ALL KEYS	SEC TEAM

Best Practice

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.

Recommended controls include, but are not limited to:

- Restricting perimeter access with walls, fences, or gates that are no less than eight feet high.
- Placing security guards or reception staff at entry and exit points
- Securing and/or enclosing external areas (e.g., base camp) as required
- Using closed circuit television (CCTV) cameras that cover all exit and entry points as well as exterior areas (e.g. front and back entrances, base camp, parking areas, loading, and unloading zones)
- Using intruder alarm systems (i.e., motion sensors and contact sensors for doors and windows)
- Lighting with full coverage outside the facility, parking areas, pathways, and all access points to decrease risk of theft, assault or other security breaches
- Installing electronic access controls with key card entry (key cards can serve dual use as ID cards)

Alternative Approach

For temporary offices and locations where installations of security systems may be impractical or cost prohibitive for the time spent, engage adequate security guards to maintain surveillance on key points of perimeter access and to provide spot checks of the perimeter.

Implementation Tip and/or Reasoning

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.

3.1.3 SHARED FACILITIES – RENTAL SPACES

LOC MGMT **SEC TEAM**

Best Practice

When sharing a facility with other businesses or productions, access to the production space(s) must be restricted to authorized production personnel, contractors and guests only.
Recommended precautions include, but are not limited to:

- Segregating work areas (e.g. construction shops) with fencing or temporary walls
- Implementing access-controlled entrances and exits that are specific to production and production spaces
- Treating all access points and borders between production-controlled spaces and common facility areas as production perimeters and implement the relevant perimeter security measures.

Alternative Approach

Review security measures and require facility landlord to provide

- segregated access for production areas from other business tenants.
- security at the standards required by the production (e.g. perimeter security with controlled access)

Implementation Tip and/or Reasoning

Do not rely on the trustworthiness of your tenant neighbors. They may have signed an NDA for their employer, but they have not signed one for the production.

Consider the landlord and the lease: the security provided, the landlord's liability versus the production's in case of a breach of the security, the maintenance and vigilance required.

Consider the improvements that should be made by the production to adequately secure the production-controlled space(s).

3.1.4 SHARED FACILITIES – VENDORS

EXEC MGMT **PROD MGMT**

Best Practice

The facilities should meet or surpass the production security policies and procedures.
In instances where vendors service multiple productions, the assets should be digitally and physically segregated from other production company assets.

Implementation Tip and/or Reasoning

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

PROD MGMT **SEC TEAM**

Best Practice

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.

Implementation Tip and/or Reasoning

Guards should regularly patrol the production perimeter and areas

3.2.2 GUARD PATROL PROCEDURES

LOC MGMT

Best Practice

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.

Patrols should monitor restricted area access but should not enter into restricted areas unless there are additional access points within which require checks or life safety risks may exist to those within.

Implementation Tip and/or Reasoning

Walk the perimeter with the assigned guard at least once to confirm their knowledge of the perimeter and its weak points. 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

PROD MGMT

Best Practice

Provide clear powers and limits of authority to security guards.

Implementation Tip and/or Reasoning

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.

3.2.4 GUARD KEYS AND ACCESS CODES

LOC MGMT **SEC TEAM**

Best Practice

Security guards should be given minimum keys or access codes to surveil the perimeters.

Security guards should not be assigned keys or codes for locks or alarms to production content or storage areas (e.g. server rooms, asset storage lockers etc.). If guards do require access to keys, their access should be logged and monitored, e.g. for life safety responsibilities.

Implementation Tip and/or Reasoning

Unless there is a point in the perimeter that is blind from outside a restricted area, there should not be a reason to provide access to a security guard.
A life safety exception may exist if activities within the restricted area are dangerous to persons within.

3.3 FACILITY AUTHORIZED ACCESS

3.3.1 AUTHORIZED ACCESS CONTROL PROCEDURES

PROD MGMT SEC TEAM

Best Practice

Productions should implement access control procedures that include, but are not limited to:

- Maintaining an updated list of individuals with access to restricted areas (e.g., editorial, art department, ...)
- Granting or revoking access privileges as needed
- Regularly updating the list so as to accurately reflect current staffing
- Limiting access to restricted areas to the fewest number of people possible (e.g., network & server room to IT personnel only)
- Access rights for contractors/third-party personnel should have a defined expiration date (e.g. end of contract)
- Contractors/third-party personnel should have supervised access to restricted areas
- No unidentified persons should be permitted in any production spaces. Visitors should be required to check-in and be issued a form of visitor ID - badge on a lanyard, sticker…
- Production staff should be trained to question individuals who lack visible production identification or to notify a person in charge of premises security.

Alternative Approach

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.

Implementation Tip and/or Reasoning

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

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.

3.3.2 PHYSICAL ACCESS CONTROLS

PROD MGMT SEC TEAM

Best Practice

Productions should implement and maintain procedures to ensure that physical access to production grounds remains secure. This includes, but is not limited to:

- All gates and fences should be secured at all times
- Doors and windows should be locked when not in use or left unattended
- All ingress/egress points should be locked at all times
- Ingress/egress points lacking a means to lock should be monitored at all times

Implementation Tip and/or Reasoning

Don't rely on production staff "common sense". Install automatic locking mechanisms wherever possible. Remind staff of the importance of locking doors.

3.3.3 ACCESS POINTS OF ENTRY – CHECK-IN/CHECK-OUT

PROD MGMT SEC TEAM

Best Practice

Personnel should be assigned to monitor points of entry to the production spaces and made responsible for supervising the check-ins and check-outs of daily hires (including Extras, Stand-ins, Crew, Specialists, Contractors, etc.) as well as guests and couriers.

All daily hires should be verified against the day's list (e.g. call sheet, extras list, etc.)

All guests should be confirmed by their host.

Every individual accessing a Restricted Access area with a keyless entry system must use their own keycard or keycode to enter. The policy "Do Not Hold the Door" should be enforced: no individual should open a door with their electronic access and allow others to pass through with or behind them unless those individuals are daily staff or visitors under the individual's supervision.

Implementation Tip and/or Reasoning

Daily and Visitor identity badges should be issued to daily staff, cast and extras, and visitors to clearly identify them as belonging on set. If this is consistently enforced, unauthorized individuals will stand out to everyone. "If you don't know them, don't let them in, direct them to the place or individual who can check them in."

3.3.4 PHYSICAL ACCESS LOGGING

PROD MGMT SEC TEAM

Best Practice

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

Alternative Approach

Call sheets and Production Reports will document the majority of on-production staff and contractors on-site each day. Similar reports can be generated for off-production (construction, etc.) staff and contractors. Check-in logs should be kept for all individuals accessing production spaces who are not logged on the daily production reports (e.g. visitors.)

Implementation Tip and/or Reasoning

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.

3.3.5 VISITOR ACCESS LOGS

PROD MGMT SEC TEAM

Best Practice

The production should keep and retain visitor logs recording check-in and check-out times and areas accessed.

Implementation Tip and/or Reasoning

Visitor logs may be kept as addendums to the daily production reports or in their own log files.

3.3.6 TEMPORARY HIRE ACCESS LOGS

PROD MGMT SEC TEAM

Best Practice

Each Daily Hire's report to and dismissal from production locations should be recorded.
Daily hires reporting off-set should be logged when checking in for their temporary ID badge and again when checking out.

Implementation Tip and/or Reasoning

Daily production reports can serve as logs provided they reflect all daily hires report and dismissal times.

3.3.7 ELECTRONIC ACCESS (KEY-LESS)

PROD MGMT

Best Practice

Access to restricted areas where assets are stored, transferred, accessed or manipulated within the production spaces, should be controlled by an access control system such as electronic swipe cards.

Secondary "backdoor" exit points which lead directly to public or common spaces should additionally have a sonic notification for egresses.

The Electronic Access control system should provide an access log. The log should map access control cards to employees and third-party personnel and be retained for the duration of production.

If issued key cards should not reference either the company or relevant access points.

Access control cards issued to third-party personnel should be easily distinguishable from those issued to employees.

Periodic inventory checks of keycards should be conducted

Keycards should only be issued to approved personnel with a legitimate business reason

Unassigned keycards should be stored in a safe location (e.g., lockbox or safe)

Alternative Approach

All entry and exit points should lock. Only authorized production employees or contractors should be issued keys (or keycards, keycodes) to open locked entries. Secondary "backdoor" entrance and exit points and areas should be locked at all times and require a key (or keycode) to enter. (See Physical Key Management and Lock Maintenance.)

Implementation Tip and/or Reasoning

Electronic access keycards can often double as identity cards.

3.3.8 PHYSICAL KEY MANAGEMENT

LOC MGMT SEC TEAM

Best Practice

Productions should implement and maintain procedures to ensure that physical keys are managed securely. This includes, but is not limited to:

- Physical keys should not unlock entryways to override electronic access control to restricted areas (e.g., server room, or editorial). If they do, an alarm should be triggered
- Periodic inventory checks of physical keys should be conducted
- Keys should only be issued to approved personnel with a legitimate business reason
- Unassigned keys should be stored in a safe location (e.g., lockbox or safe)
- Master keys should only be issued to approved personnel with a legitimate business reason
- Distributed master keys should be tracked and have a check-in / check-out process
- Keys should be inventoried and accounted for on a regular basis
- Issue ‘restricted’ / ‘do not copy’ keys

Implementation Tip and/or Reasoning

Don't be flippant about the keys to the kingdom. Your perimeter is your first line of defense, the keys to that perimeter are your first point of weakness.

3.3.9 LOCK MAINTENANCE

LOC MGMT	SEC TEAM

Best Practice

Locks should be changed in the event that a key is lost or stolen. All lock changes information should be documented, including but not limited to who made the change and when the change occurred.

Implementation Tip and/or Reasoning

A lost or stolen key is a "security incident" and should be responded to quickly and appropriately.

3.3.10 USE OF PORTABLE DIGITAL DEVICES WITHIN RESTRICTED AREAS

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

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. Guidelines for use of digital devices include, but are not limited to:

- If an exception has been approved that permits use of digital devices in restricted areas, use of those devices should be strictly monitored
- Provide ID badges which clearly identify personnel and third parties permitted to use digital devices in restricted areas
- Provide a check-in and check-out station for personnel to declare restricted devices.
- When accessing highly sensitive areas, production crew and contractors should be searched for devices, as appropriate
- A facility for storing prohibited devices while personnel visit the restricted areas should be provided
- Tamper-evident stickers should be used on digital recording devices to prevent the use of cameras where applicable
- Prohibition signs on use of digital devices should be clearly visible in and around restricted areas

Alternative Approach

Prohibition signs on use of digital devices should be clearly visible in and around restricted areas. Require personnel and third parties to declare all digital devices they are carrying

Provide ID badges which clearly identify personnel and third parties permitted to use digital devices in restricted areas.

Implementation Tip and/or Reasoning

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.

3.4 LOCKED STORAGE AND SAFES

3.4.1 LOCK-UPS, VAULTS AND SAFES

PROD MGMT **SEC TEAM** **IT**

Best Practice

Sensitive assets, information and content housed on physical media (e.g. servers or portable hard-drives) should be stored in a secured location (e.g. vault or safe). Guidelines for such vaults or safes include, but are not limited to:

- The vault should be access-controlled. Electronic access control is preferred
- Access to the combination or key should be limited to a highly restricted list of employees
- Motion activated CCTV of enclosed vault space, recordings maintained for duration of production
- A vault inventory should be maintained including the status of each asset (e.g., date/time signed in/out, recipient name and signature)
- Access to the vault combination or key should be kept to a highly restricted list of employees
- The safe / vault should always be locked when not in use
- The combination / key to the vault should be changed after an employee with access has departed or been terminated
- The production should implement and maintain policies and procedures to access / unlock vault after hours.

Alternative Approach

When CCTV is not feasible, be sure the vault or safe is supervised at all times.

Implementation Tip and/or Reasoning

Place lock-ups, vaults and safes in easily secured locations, in clear view of workstations or within restricted areas.

3.4.2 SAFE SPECIFICATIONS

PROD MGMT

Best Practice

Specifications for safes include, but are not limited to:

- Should be large enough to fit all anticipated items requiring safe storage (e.g. editorial portable hard drives, accounting cash and check stock)
- Any safe weighing less than 300 lbs. should be securely bolted to the floor or wall
- Should be kept locked at all times
- Should have a minimum fire rating of 30 minutes

Implementation Tip and/or Reasoning

Choose a safe that is appropriately difficult to open and/or remove from the premises: easy for those authorized so they won't be tempted to just leave it open, difficult for those unauthorized to deter break-in or removal.

(RETURN TO TABLE OF CONTENTS)

IV. ASSET MANAGEMENT

4.1 PSEUDONYMIZED SECURITY TITLE

4.1.1 USE OF ALIAS TEMPORARY TITLES

EXEC MGMT	PROD MGMT

Best Practice

Unless restricted by local law (AKAs, aliases, or code names) Alias Temporary Titles should be used to protect the production’s anonymity in tracking systems, shared storage, and on physical assets.

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

There should be clear documentation to associate all assets labeled with the Temporary Title to the legal Title as part of the chain of title evidence.

Implementation Tip and/or Reasoning

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.

The legal Title(s) are the release title(s) and/or the title of the material originally purchased or licensed to produce.

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

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

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

Content management systems, inventory databases, or asset logs should allow users to designate specific items or data as "high security."

"High security" assets should be flagged for easy production identification without obvious labelling for unauthorized recognition (e.g. color-coded labels, segregated storage)

Implementation Tip and/or Reasoning

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 "Hight security" treatment than one may think.

4.3 INVENTORY POLICIES

4.3.1 RECORDING CHAIN OF CUSTODY

PROD MGMT   SEC TEAM   IT

Best Practice

A chain of custody planned pipeline should be established for digital and physical assets containing content or protected or confidential information.   The plan should include

- Point of acquisition and/or creation
- Initial custodian
- Point of transfer(s) – reason, time, and/or place
- Downstream custodian(s)
- Methods of transfer(s)
- Authority to transfer
- Verification of successful transfer

Movement records should be maintained for the duration of production (check-in/check-out log sheets, computer systems log files.)

Movement of assets at a minimum should capture:

- Date / Time
- Custodian
- Origin (including creation)
- Destination

Implementation Tip and/or Reasoning

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.

4.3.2 INVENTORY MAINTENANCE

PROD MGMT SEC TEAM IT

Best Practice

The chain of custody of physical and digital assets should be maintained via inventory database, spreadsheet, or content management system (i.e., a log of content that is created or acquired by a production department, transferred between departments, delivered to 3rd party facilities, damaged or destroyed.)

Implementation Tip and/or Reasoning

Promote a habit of recording receipt and release of physical assets including digital assets moved via portable devices or transfer services within each department to create a sense of responsibility for the assets whilst in the department's possession.

There are asset management and barcoding tools readily available and easy to implement which can centralize the tracking across departments, or simple excel spreadsheets, even paper logs.

Digital asset access and movement may be tracked by automated logging systems.

4.3.3 INVENTORY PIPELINE & LOG ACCESS

PROD MGMT SEC TEAM IT

Best Practice

Access to inventory system logs, databases, spreadsheets, and paper logs should be restricted based on the concept of least privilege. This includes, but is not limited to:

- Purchase order logs
- Shipping logs
- Inventory lists
- Asset pipeline outlines, summaries, plans
- Schedules and calendars relating to pipeline

Implementation Tip and/or Reasoning

Protecting the information related to what and where assets are located and how they are moved is a key step in preventing unauthorized access. It is critical to create the lists and logs and plans, but these inventory records are themselves confidential information.

4.4 ASSET TRACKING

4.4.1 LOGGING & TRACKING

ALL KEYS SEC TEAM

Best Practice

Productions should ensure secure handling of all physical assets and content creation, storage and transport. Guidelines include, but are not limited to:

- Assets and Content should be immediately identified, tagged, tracked and stored securely upon acquisition or creation
- Assets and Content should be labeled with a unique identifier and controlled by an inventory or content management system
- Assets and Content should be tracked as it is transferred between custodians (e.g. from set to production, from production to editorial or lab, from designers to manufacturers, etc.)

Implementation Tip and/or Reasoning

Provide the crew with a simple system upfront (stickers, barcode printers, paper log-sheets, excel spreadsheet forms, or asset management software) and make it a daily regular requirement of their workflow.

4.4.2 DIGITAL ASSETS ON PORTABLE OR LOCAL DEVICES (THEIR PHYSICAL FORM)

PROD MGMT SEC TEAM IT

Best Practice

A documented process for checking out digital content onto portable devices or local computers should be established. Guidelines should include, but are not limited to:

- Ensuring that checkout durations not exceed 24 hours or the duration of the custodian's shift unless explicitly approved in writing by management (e.g. all work should be stored to the secured shared storage and removed from local or portable devices at the custodian's end of shift.)
- Performing regular inventory checks to track content and investigate individuals who have not returned content in a timely manner.
- Using automatic system notifications to alert team members when content has not been returned within the expected timeframe.
- Content should be deleted from portable devices as soon as purpose for storage on portable device is completed.

Portable and Local Devices (e.g. USB sticks, portable hard-drives, flash drives) which are used to store, backup or transport sensitive information (e.g. financial, design and content) should be logged, tracked and secured. See related guidelines.

Implementation Tip and/or Reasoning

As an alternative to crew holding digital assets on portable devices or local computers (physical assets which require physical security), provide the crew with simple means to store and retrieve digital assets from a secured shared server mapped to their computer.

Checking out digital assets is no different from extras checking out props. We have traditionally kept check-out and check-in logs for physical assets and should extend the same practices to all assets - including digital assets.

Limit the number of individuals empowered to check out digital assets (files, content).

Establish clear individual responsibilities for tracking digital assets checked-out through check-in.

Set reminders to check on returns.

4.5 PEOPLE ARE ASSETS

4.5.1 SECURITY FOR THE TEAM

PROD MGMT

Best Practice

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.

Implementation Tip and/or Reasoning

Securing the team is an extension of securing the production.

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.

4.6 PHYSICAL ASSETS – SECURING, STORAGE, SHIPPING

4.6.1 SHIPPING AND RECEIVING POLICIES

ALL KEYS SEC TEAM

Best Practice

Productions should maintain policies and procedures specifically devoted to shipping and receiving. Guidelines include, but are not limited to:

- Requiring that a signature be obtained at the point of shipping
- Keep receipts or copies of shipping bills of lading or airbills
- Reconciling the identity of every courier / delivery person against the corresponding work order
- Verifying the quantity and descriptions of packages against shipping documents

Implementation Tip and/or Reasoning

The best time, the only time, to check the paperwork and inventory shipped or received with a shipping vendor is at the moment when the items change custody between the shipping vendor and the production. Discovering discrepancies later may remove any loss liability from the vendor.

4.6.2 SHIPPING PACKAGING

ALL KEYS SEC TEAM

Best Practice

Prior to shipping, content should be packaged using secure, tamper-proof or tamper-evident pouches or containers.

Implementation Tip and/or Reasoning

Tamper-proof or tamper evident packages provide a deterrence to curious inspection and evidence in the case a package has been opened in transit.

4.6.3 SHIPPING PACKAGE LABELING

ALL KEYS SEC TEAM

Best Practice

Actual title information should never be visible on the outside of packages.

- Unless required, no title should be visible on the outside of packages.
- When a title is required, use security titles (code names or aliases)

Implementation Tip and/or Reasoning

Packages should travel as anonymously as possible in order to avoid curiosity or opportunistic theft.

4.6.4 STAGING AREA MONITORING

PROD MGMT

Best Practice

Permanent shipping & receiving areas, e.g. loading docks, should be monitored at all times assets or content are collected and staged for shipping. If the staging area is out-of-eyesight of a manned workstation, camera surveillance should be used. When used, notifications of camera surveillance should be posted.

Alternative Approach

Establish shipping and receiving staging areas which are adjacent to work stations and under continuous human observation or to which access is restricted by locked doors and only opened by production personnel for the purpose of staging or transferring for shipping and/or receiving.

Implementation Tip and/or Reasoning

Assets and content should not be left unattended while awaiting shipping. They should remain protected at all times while in the control of production.

4.6.5 DAMAGES, LOSSES & DISCREPANCIES OF SHIPPED ASSETS

ALL KEYS SEC TEAM

Best Practice

Losses, discrepancies or damage to shipped goods should be immediately reported to the department head and/or production manager.
Lost or damaged assets should be logged on the asset inventory.
Lost or damaged assets are a “security breach.”
Shipping method should be reviewed per the incident response guidelines.

Implementation Tip and/or Reasoning

While a shipping discrepancy, loss or damages may be unintentional, they are still a form of breach. Those responsible for the assets and for the policies for managing them should review the shipping method to avoid a future reoccurrence.

4.6.6 COURIER AND SHIPPING RECEIPTS/LOGS

ALL KEYS **SEC TEAM**

Best Practice

Retain for the duration of the production all courier and shipping company bills of lading, airbills, pick-up and delivery receipts.

Record each custodial transfer (to or from the courier or shipper) on the asset inventory tracking log.

Shipping and receiving receipt/logs should include shipping and receiving completed by production employees, contractors, couriers and shipping services.

The information recorded in shipping logs should include, but not be limited to:

- Time of shipment
- Sender's name and signature
- Recipient's name
- Address of destination
- Tracking or airbill number from the courier
- Corresponding purchase or work order
- Courier's name and employee ID number (if applicable)

Implementation Tip and/or Reasoning

Keep a file for every courier, shipper, vendor delivery service and retain all documents related to their services. If records are electronic (e.g. email confirmations), save them to a digital file folder.

4.6.7 CLOSED OFFICE HOURS / OVERNIGHT DELIVERIES

PROD MGMT **SEC TEAM**

Best Practice

Productions should implement and maintain policies and procedures to securely receive and handle off-hours/overnight deliveries of content (e.g. the day's rushes from set).

Implementation Tip and/or Reasoning

Provide a secured location (e.g. locking parcel drop boxes) or overnight security guard to receive content deliveries during closed office hours. Provide a means to report the drop off such as a log sheet.

4.6.8 PORTABLE AND LOCAL DEVICES & COMPUTERS

EXEC MGMT **ALL KEYS** **SEC TEAM** **IT** **3RD**

Best Practice

Portable devices (e.g. USB sticks, portable hard-drives, flash drives) which are used to store, backup or transport sensitive information (e.g. financial, design and content) should:

- never be left unattended and unsecured (i.e., open or visible upon vacated desks).
- be encrypted (e.g. password protected) using hardware-based encryption using a current vetted algorithm such as AES 256-bit key size.
- when not in use, should be kept in locked storage.
- Data should be stored temporarily and deleted from devices as soon as useful purpose for storage is completed. See paragraph *4.9.2 Destruction of Content*.

Implementation Tip and/or Reasoning

Supply secure portable devices which offer built-in encryption.

Supply convenient lock-ups for portable devices.

4.6.9 INVENTORY COUNT PROCEDURE

ALL KEYS SEC TEAM IT 3RD

Best Practice

Inventory count procedures for physical assets should adhere to the following guidelines:

- Include all assets: equipment, props, costumes, designs, etc. as well as physical data discs, masters, tapes, film, and hard drives in all inventory counts
- Utilize an inventory management system to record and track all digital content and content that is received electronically
- Performing weekly inventory counts for vendors holding inventory (e.g. film labs, or contractors providing props, prosthetics, wardrobe etc. which are manufactured for and the assets of the production.)
- Where possible, create separation of duties: personnel responsible for maintaining inventory should not be responsible for counting inventory
- Procedures for inventory count shortages and overages of physical assets, in particular assets containing content such as portable hard-drives should be communicated to employees via policy and/or training. Shortages and/or overages should be reported and resolved as soon as is possible.

Alternative Approach

Frequent spot checks of all physical assets against inventory lists.

Require vendors holding inventory to submit updated inventories any time there is a change or at least weekly. Spot check for veracity. (Trust but verify.)

Implementation Tip and/or Reasoning

Without an inventory and an inventory count procedure, losses can go undetected for long periods of time. The longer the time from the date of the loss until its detection, the more difficult it will be to investigate.

4.7 DIGITAL ASSETS

4.7.1 DIGITAL ASSET MANAGEMENT (DAM) POLICY

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

DAM system policies and procedures should be communicated to all users. These procedures include, but are not limited to:

- Digital assets (content) should be tracked and monitored with logs and notifications when it is transferred to or from external sources and accessed
- Digital content should never be transferred via email, transfers when necessary should be via approved Data Transfer services, see "Content Transfer System Guidelines".
- Digital content should not be stored or accessed offsite with the exceptions of:
  - secure and encrypted backup data
  - secure and encrypted cloud services for digital asset management and content streaming, see "Use of Cloud Services".
- Digital content should be properly labeled (file name, storage location).
- Access rights to digital content should be assigned based on policies of "least privilege."
- Digital asset inventory and access logs should be maintained at all times.
- Create clear data asset storage and filing system: where data should be stored, the folder or tagging labels that should be applied, and the file naming.
- Create a file naming convention for the production which will organize files into easily searchable lists. Examples:
  - Type Driven:
    - "Document Type/Key Identifier – Date (YEAR-MM-DY) – Version#"
    - "Callsheet-1stUnit-2018-01-03-Day1"
    - "DayPlayer-Smith-2018-01-03-fullyexecuted"
    - "VFXAsset-CharacterXYZ-vABC001
  - Date Driven
    - "Date (Year-MM-DY) – Document Type/Key Identifier – Version#"
    - "2018-01-03-DailyProductionReport-Day1-Approved

Implementation Tip and/or Reasoning

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.

Lost files due to disorganization and misnaming are frequent causes of data asset losses. A shared system and policy are easier to teach, makes searches easier, and makes identifying mislabeled data files easier.

4.7.2 DIGITAL ASSET COPIES

	PROD MGMT	SEC TEAM	IT

Best Practice

A single copy of digital assets should exist locally and be stored on the appropriate Restricted Access production network shared storage SAN or NAS or on an encrypted external hard drive. Additional copies of digital assets should be prohibited. (Backup and archive copies excepted.)

Alternative Approach

Minimize the number of copies of all digital assets.

Implementation Tip and/or Reasoning

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

EXEC MGMT	PROD MGMT	SEC TEAM	IT

Best Practice

Email

All production generated email should be sent from a production-controlled email domain.

All production staff who generate emails should be provided a production email account, it is also recommended that production staff who will regularly receive email communications be issued production email accounts.

A policy of email backup, journaling, archiving, retention duration and deletions should be established per the advice of production counsel.

If available, implement email service data loss prevention services to encrypt and track emails and attachments. If implemented, provide policy and use training to all email users.

A policy of "zero attachments" and sharing of files via "links" should be implemented.

Instant Messaging

All production instant messaging should be sent from a production-controlled instant-messaging or chat service with a closed recipient list limited to authorized production team members.

A policy of message backup, journaling, archiving, retention duration and deletions should be established per the advice of production counsel.

If available, subscribe to an encrypted messaging service

A policy of "zero attachments" and sharing of files via "links" should be implemented.

Implementation Tip and/or Reasoning

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 are used. Additionally, when personal communications services are used the individual is in possession of those work product communications which are owned by the 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 or cancelled as needed.
- If email and email attachment encryption are available, enforcing their use is recommended. Of equal importance is encrypting 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.

4.8.2 COMMUNICATION DISTRIBUTION LISTS

PROD MGMT SEC TEAM IT

Best Practice

Many communication tools use distribution lists to group many recipients into a single communication (e.g. group email address), if used the following guidelines should be followed:

- Review the recipient member list prior to sending a group communication
- Review distribution lists to add or remove temporary list members
- Create separate distribution groups for permanent (e.g. run-of-production or run-of-group-distribution) members and distribution groups for temporary members (e.g. short-term or daily hires)
- Use the BCC to hide member emails from each other (particularly if personal email addresses are included and privacy regulations apply.)
- If using email data loss protection tools, prior to sending convert the group email address to the full email address list in order for the tools to track the recipients.

Implementation Tip and/or Reasoning

Distribution lists save the production office time, use some of that time to carefully manage the lists.

4.9 SECURE ASSET & DATA DESTRUCTION

4.9.1 DAMAGED STOCK CONTAINING CONTENT

PROD MGMT SEC TEAM IT 3RD

Best Practice

Rejected, damaged, and obsolete stock containing content should be securely erased, degaussed, shredded, or physically destroyed before disposal.
If performed by a third-party, a certificate of destruction should be presented upon completion of services.

Implementation Tip and/or Reasoning

See “Destruction of Content"

4.9.2 DESTRUCTION OF CONTENT

PROD MGMT SEC TEAM IT 3RD

Best Practice

The destruction or recycling of media containing assets should follow leading practices as outlined in the National Institute of Standards and Technology (NIST) media sanitization standards (SP 800-88). For more information about destruction of content visit:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Alternative Approach

Engage a service which provides secure media destruction / erasure.

Implementation Tip and/or Reasoning

Deleting all and drive reformatting does not completely erase all data from the drive. There are specialized methods and technologies for complete erasure by degaussing and data overwriting.

4.9.3 FINISHED ELEMENTS

EXEC MGMT	**ALL KEYS**	**SEC TEAM**	**IT**	**3RD**

Best Practice

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.

Access to finished elements should be restricted based on policies of least privilege until such time as they are destroyed.

Implementation Tip and/or Reasoning

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.

4.9.4 STAGING FOR RECYCLING & DESTRUCTION

	ALL KEYS	**SEC TEAM**	**IT**	**3RD**

Best Practice

Elements being staged for recycling or destruction should be stored in a secure location. The following guidelines should be adhered to at a minimum:

- Rejected, damaged, obsolete stock, or finished elements should be clearly labeled "TO BE DESTROYED or RECYCLED - DO NOT USE"
- Rejected, damaged, obsolete stock, or finished elements should be segregated from other types of content and materials
- Rejected, damaged, obsolete stock, or finished elements should be stored in locked disposal bins
- Rejected, damaged, obsolete stock, or finished elements should be stored a minimum amount of time before recycling or destruction

- Rejected, damaged, obsolete stock, or finished elements should be stored in a restricted, secure area (e.g., a vault or safe) prior to recycling or destruction

Implementation Tip and/or Reasoning

Treat assets to be destroyed as protected assets until they are destroyed. Many a hack and embarrassing theft has been achieved by sifting through the garbage.

4.9.5 THIRD PARTY DESTRUCTION OF CONTENT

PROD MGMT	SEC TEAM	IT	3RD

Best Practice

Destruction of physical media containing content by a third-party vendor should adhere to the following requirements:

- Destruction of content should be performed on site
- This process should be overseen by a production employee
- A certificate or record of destruction should be provided for each completed job

Alternative Approach

If destruction of content by a third party must occur offsite, make the content unrecognizable and anonymous, e.g.:

- damage beyond recognition physical content assets,
- delete all digital content assets
- anonymize all labeling, remove any reference to title or company

Implementation Tip and/or Reasoning

Do not rely on content being destroyed without someone to observe the destruction.

4.9.6 DESTRUCTION OF ASSETS LOGGING

ALL KEYS	SEC TEAM	IT	3RD

Best Practice

Destruction of physical and digital assets and content should be logged and recorded on inventories.

Implementation Tip and/or Reasoning

A log of all destroyed assets (physical and/or content) should be maintained and included in the inventories.

(RETURN TO TABLE OF CONTENTS)

V. VIRTUAL – DATA – SECURITY

5.1 LOCAL AREA NETWORK (LAN), WIDE AREA NETWORK (WAN) AND INTEROFFICE CONNECTIONS

5.1.1 NETWORK DIAGRAMS

PROD MGMT	IT

Best Practice

Detailed network and infrastructure diagrams including WAN, DMZ, LAN, WLAN (wireless), VLAN, firewalls and server/network topology should be created and kept up to date. WAN documentation that describes and illustrates the number of connections to and from the facility, other facilities and the cloud should also be included.

Implementation Tip and/or Reasoning

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 and if appropriate the internet.

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.

5.1.2 POINT-TO-POINT CONNECTIONS (DATA TRANSFER CHANNELS)

PROD MGMT	IT

Best Practice

All point-to-point (e.g., VPN, private fiber, etc...) connections used by the production through which content travels should be documented and reviewed for usage and business validity at setup and frequently thereafter.

Alternative Approach

Review the connections at least every 6 months, 3 months recommended.

Implementation Tip and/or Reasoning

Particularly check whether the need remains, who has access and what data (content) it is used to transfer.

5.2 FIREWALL AND SECURITY SERVICES

5.2.1 FIREWALL GUIDELINES

PROD MGMT	IT

Best Practice

A stateful inspection firewall should be in place for all internet connections to prevent unauthorized access to computers and internal networks. For protection of infrastructure handling sensitive content, physical firewalls should be implemented.

Firewall policies should explicitly block all unauthorized / unapproved ports and protocols. At minimum, the baseline configuration should:

- Block internal addresses over external ports
- Deny insecure protocols to and from the production network
- Block use of unused ports and services

The following requirements should be met when setting up the firewall:

- Administrator to be alerted when certain conditions are met (e.g. anomalous traffic behavior, bandwidth threshold exceeded)
- All traffic logs are enabled
- All protocols to be denied by default and only specifically required protocols to be allowed

Alternative Approach

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.

Implementation Tip and/or Reasoning

The firewall is an essential component of the 'data perimeter'.

5.2.2 FIREWALL MANAGEMENT

	IT

Best Practice

Firewall management policies and procedures must be documented, and at a minimum, cover:

- Provisioning requirements (i.e., based off the concept of least-privilege)
- Deployment requirements (e.g., baseline requirements)
- Change control requirements (e.g., Patching, Upgrades, Firewall Rule management)
- Monitoring (e.g., periodic review of ACLs and baseline configuration)

Firewalls should be configured to actively alert security members of key security events, and should, at a minimum, meet the following requirements:

- Security events tagged for audit should generate an alert to be sent to the firewall administrator or Security team
- The firewall administrator should review the alert in a timely manner based on the severity of the incident as documented in the Security or Incident Response policy
- Findings from all investigations should be documented
- Corrective actions should be taken to prevent malicious traffic

Firewalls, at a minimum, should support the following:

- Basic Border Gateway services (e.g., Gateway AV, IDS/IPS, URL Filtering) should be enabled
- Based on severity, events tagged for audit should generate an alert.

An intrusion detection / prevention system (IDS / IPS) that includes, but is not limited to the following should be implemented for the Production network:

- The IDS / IPS should have a subscription to antivirus and intrusion detection updates. Updates should occur no less than weekly
- All changes to the IDS / IPS rule set should be authorized by onsite security representative / team and documented. There should be an audit log of all changes performed on the IDS / IPS.

The IDS / IPS administrator should review alert events immediately and document findings from all investigations. Corrective actions should be taken to prevent malicious traffic.

5.2.3 SEGREGATION

IT

Best Practice

WAN connection should be segregated using dedicated software or hardware firewalls. Firewall rules / ACLs should be configured to deny all traffic to any internal network except for explicit hosts that reside on the DMZ. Routes to network segments used to manage / store content should be disabled.

5.2.4 EMAIL FILTERING

IT

Best Practice

Email filtering software or appliances should be setup to prohibit:

- Phishing emails
- Known domains that are sources of malware and viruses
- Executable attachments (i.e. Visual Basic scripts, .exe files etc.)

- Attachments larger than 10MB

Do not assume email filtering software or appliances 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.

Alternative Approach

The only alternative is employee training to spot phishing emails.

Implementation Tip and/or Reasoning

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

5.2.5 WEB FILTERING

IT

Best Practice

Web content filtering software or appliances should be setup to prohibit:

- Unauthorized file sharing sites
- Known sites for malware, viruses, hacking, or any other malicious activity

Alternative Approach

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

5.2.6 DNS POLICIES

IT

Best Practice

A secure DNS infrastructure that comprise of the following should be implemented:

- DNS forwarders
- Caching-only DNS servers
- DNS advertisers
- DNS resolvers

Other DNS guidelines include, but are not limited to:

- Configuring the DNS to prevent cache pollution
- Configuring DNS to utilize approved forwarders
- Enabling DDNS for secure, trusted connection
- Using firewalls to control DNS access

- Setting access controls on DNS registry entries
- Setting access controls on DNS file system entries

5.2.7 LAN SECURITY

PROD MGMT	IT

Best Practice

Network segregation between the production networks should be implemented (e.g. guest, production office, accounting, art/design, and editorial, should be on separate networks). Department Networks which host digital content should not access the internet. Computers with legacy applications which rely on older operating systems should be segregated from all other production computers on an isolated network.

Security measures on each LAN should include, but are not limited to:

- Authentication
- Access Control List (ACL)
- VLANs
- Internal Firewalls
- SNMP v3 or higher, see paragraph 5.2.8 Simple Network Management Protocol
- Logging
- Segregation by physical Air Gap, or logical segmentation via Layer 2 VLAN, or via Layer 3 VLAN
- Access to each LAN should be limited to the users with specific business needs for access.
- For Wi-Fi LANs - the access passwords should be issued to authorized users only. NO Wi-Fi passwords should be posted visibly with the sole exception of the Guest Wi-Fi which in turn should only provide access to the internet.

Implementation Tip and/or Reasoning

Office networks should be setup 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.

5.2.8 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

	IT

Best Practice

SNMP should be disabled for read-and-write access if it is not in use.

For SNMP usage, the following should be implemented:

- SNMP v3 or higher
- Strong passwords for SNMP community strings, different from those used for administration or authentication credentials

Access to devices using SNMP should be restricted via ACLs to only authorized management systems in a trusted management zone.

Implementation Tip and/or Reasoning

SNMP is for connecting peripheral equipment such as routers, printers etc.

5.3 PRODUCTION NETWORKS

5.3.1 PRODUCTION NETWORK RESTRICTIONS

PROD MGMT	IT

Best Practice

LAN, WAN, WLAN Networks should be segmented to isolate access (e.g., Production, Editorial, Art-Design, DMZ, Guest) via the following methods:

- Physical Air Gap
- Logical segmentation via Layer 2 VLAN
- Logical segmentation via Layer 3 VLAN

Networks should be identified as Restricted Access, General Access, Guest/Visitor Access in the same manner as locations and facilities will have restricted access areas versus general production access areas and public common areas.

Implementation Tip and/or Reasoning

Restricted Access network segments should be isolated from General Production Access network segments and Guest/Visitor network segments using, at minimum, per the following guidelines:

- Define Access Control Lists that explicitly allow access to the content/Restricted Access network from specific hosts that require access (e.g., anti-virus server, patch management server, content delivery server, etc.)
- Include explicitly defined ports and services that should allow access in the Access Control Lists
- Segment or segregate networks based on defined security zones
- Implement firewall rules to deny all outbound traffic by default and explicitly allow specific systems and ports that require outbound transmission to designated internal networks, such as anti-virus definition servers, patching servers, content delivery servers, licensing servers (only when local licensing servers are not available), etc.

- Implement firewall rules to deny all inbound traffic by default and explicitly allow specific systems and ports that require inbound transmission from designated content delivery servers.
- Assign static IP addresses by MAC address on switches
- Disable DHCP on the content/Restricted Access network
- Prohibit any production computer system from connecting to more than one network at a time
- Prohibit content from being used or stored in General Production Access or Guest/Visitor networks

5.3.2 INTERNET ACCESS RESTRICTIONS

PROD MGMT	IT

Best Practice

Restricted Access networks storing content or confidential data (Editorial, Design, VFX, Accounting, etc.) should not access the internet directly unless a business case requires it. Preferred access methods are via:

- A separate Data I/O network isolated from the Restricted Access network(s)
- A remote hosted application / desktop session
- A keyboard / video / mouse (KVM) solution
- Access granted exclusively to whitelisted external IP address or URL and specific port to access sites that provide software license validation and software upgrades (provided there is no other possible way of performing the software license validation and upgrade) - access is disabled immediately after use.

The following restrictions apply to the approved access methods:

- Drives should not be mapped remotely to the Restricted Access network
- Printer mapping on the remote host should be disabled
- The ability to mount removable media on the remote host should be disabled
- Where system functionality permits, copy / paste and file-transfer abilities should be disabled
- Remotely hosted applications and remote desktop sessions should be encrypted
- Devices should be physically disconnected from the Restricted Access network and physically moved and connected to the Data I/O network. Technicians should complete anti-virus and malware scanning before adding the system back to the Restricted Access network.
- Proxy license services should be hosted internally and within service area of the network

Implementation Tip and/or Reasoning

Create multiple distinct and separate networks. Workflow requirements should determine which networks access or do not access the internet. Workstations storing content should connect to networks with no internet access and should not share any local storage or service with workstations connected to networks accessing the internet.

5.3.3 CONTENT TRANSFER NETWORK

IT

Best Practice

Content Transfer or Data I/O networks should be located between external connections and the production networks, segregated logically by firewalls or switch ACLs. This network hosts machines/systems used to download or deliver content (e.g., Content Transfer Systems). Guidelines on network access to and from the Content Transfer Systems include:

- Content transfer systems are allowed to pull content from external systems or receive content pushed by external systems
- Content transfer systems are allowed to push completed content to external systems or accept connections from external systems to pull completed content
- Content transfer systems should not be allowed to connect to internal systems
- Internal systems are allowed to connect to the content transfer systems to pull client content or push completed content
- All access to and from content transfer systems should be restricted to specific servers and services.

5.3.4 DATA I/O (INBOUND/OUTBOUND) ACCESS

IT

Best Practice

Network access from Restricted Access networks to Data I/O network should be highly restricted. A unidirectional workflow should be setup to allow production users to pull data from a write-only inbox that has been received by Data I/O teams who share in the Data I/O network segment. Like-wise a unidirectional workflow that allows production users to push data from a read-only outbox to Data I/O should also be set up.

Any production system or ports that require outbound or inbound transmission to a designated Data I/O network should be explicitly defined in a firewall rule or ACL as a unidirectional push from production to Data I/O or a pull from Data I/O into production.

Alternative Approach

Hardware-encrypted hard drives using AES-256-bit encryption should be used to transfer data between Restricted Access networks and Data I/O systems when production and Data I/O networks do not have any connections and are different, physically separate VLANs.

5.3.5 SWITCHING

IT

Best Practice

Access to content / production systems should be restricted from unauthorized access through the implementation, at a minimum, of the following security protocols:

- Inactive switchports should be disabled on networking equipment
- Port security should be enabled
- Use of physical Ethernet cable locks
- The use of non-switched devices such as hubs and repeaters on the perimeter of the network should be prohibited.

5.3.6 DUAL-HOMING / BRIDGING SEGREGATED NETWORKS

IT

Best Practice

Restricted Access network(s) should have measures implemented on the LAN to prevent computer systems from "bridging networks" or connecting with more than one network. Best practices include, but are not limited to:

- The server blade chassis should not have hot-swapping ability enabled for network interfaces (e.g., HPVPLEX or Cisco B22)
- The server blade chassis should not have access to both the Data I/O networks and Restricted Access networks at the same time (i.e. spanning across two different network domains)
- Server blade systems should not have physical connectivity to the Data I/O networks and Restricted Access networks at the same time. Different network or storage interfaces should not be provisioned to the same blade chassis

EXEMPTION: Systems that require connectivity to a like production and a metadata network (i.e. Stornext) may be exempted from the bridging exclusion.

5.4 WIRELESS NETWORKS

5.4.1 WIRELESS NETWORKS GENERAL

IT

Best Practice

Guidelines for General Production Access wireless networks include, but are not limited to:

- Wireless network SSIDs should not contain any identifiable information (e.g., the company name, phone number or project title or security title)
- Wireless networks should route users directly to the intended production network only (e.g., Guest wireless network to the Internet only, Restricted Access Wireless networks to the equivalent Restricted Access LAN.)
- Do not post Wi-Fi passwords publicly. They should be provided to authorized users only and kept at all times confidential.

5.4.2 PRODUCTION WIRELESS NETWORKS

IT

Best Practice

Guidelines for wireless networks in production environment include, but are not limited to:

- Restricted Access wireless networks should not provide access to any General Production Access network and Guest/Visitor network but production local Restricted Access networks only. Firewall should be used to segregate these networks and restrict access by specific servers and services.
- The SSID should not contain any identifiable information (e.g., the company name or phone number)
- Wi-Fi Protected Setup (WPS) should be disabled if applicable
- MAC address filtering should be enabled
- Production wireless networks should not share any infrastructure with other existing wireless networks. This refers to access points, data connections, routing, and authentication services
- The IP addressing range should not be shared with any other environment
- A centralized wireless access solution should be configured to scan the network daily to alert administrators of rogue wireless access points upon detection
- Systems approved to access Production wireless networks should not possess the ability to bridge Production and General Production Access network networks
- Where possible, certificate-based authentication of devices accessing production network should be enabled.
- The Wi-Fi SSID or passwords for the Production network(s) should not be shared, if possible. IT should provide the WI-FI password directly to each endpoint approved to access a production network.

Implementation Tip and/or Reasoning

Generally, the Wireless networks should adhere to the same guidelines as the Local Area networks. See “Production Networks”.

5.4.3 PRE-SHARED KEY (PSK) USAGE AND AUTHENTICATION IN PRODUCTION WI-FI NETWORKS

IT

Best Practice

Access to Production network via Production wireless network should require 2-step authentication:

- Unique PSKs dynamically assigned over Production network and installed in an approved computer to join Production wireless network.
- Two-factor VPN authentication to access Production network
- Configuration of PSKs should include but not be limited to the following guidelines:
- Using WPA2 with CCMP (AES) encryption
- Requiring a complex passphrase that changes occasionally and at a minimum when key company personnel (e.g., administrators, users with the knowledge of the network and authentication systems) are terminated
- Revocation of WPA2-PSKs when an approved computer is stolen, lost, or when user accounts are disabled

5.5 SHARED STORAGE, SAN AND NAS SERVERS

5.5.1 LOCAL DATA STORAGE - SAN / NAS SECURITY

IT

Best Practice

Storage devices should, at a minimum, abide to the following guidelines:

- Enable ESP
- Ignore name server requests from unauthorized FC devices
- Restrict automatic E-Port replication
- Restrict Super User privilege on client computers
- Utilize DES Authentication for RPC
- Encrypt Client / Server timestamp

Server security, including SAN and NAS volumes, should include, but not be limited to:

- Antivirus protection
- Secured ports and services
- Use of standard configuration / image servers

- User access should be linked into central administration systems (See section *5.10 Privileged Access Management*.)
- Internet access on shared storage devices should be disabled with the exception of mission critical services required for performance and security activities. All outbound traffic must be whitelisted and filtered through a proxy.

5.5.2 SEGREGATION OF STORAGE

PROD MGMT SEC TEAM IT

Best Practice

The storage of content and confidential data should only reside on the restricted access networks (e.g., not in general access or guest environments). Storage should not span across segregated networks (e.g., bridging networks).

Implementation Tip and/or Reasoning

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

5.6.1 CONTENT TRANSFER POLICIES & PROCEDURES

PROD MGMT SEC TEAM IT

Best Practice

Policies and procedures for content transfers should be developed and maintained. Such policies and procedures should include, at a minimum, the following:

- Creating an approval process to authorize the transfer of content
- Creating and maintaining a list of users who are responsible for transferring content to and from the production network
- Creating and maintaining a log of recipients (within the production or 3rd parties) to which content is digitally transferred for additional service fulfillment or storage. The log should include the recipient's name, address, key contact person, phone number, and email address

- Tracking which machines are dedicated servers / workstations for transferring content and noting the location of these machines
- Using an approval process that checks for proper authentication
- Conducting regular reviews of who may access the transfer services. This includes, but is not limited to, removing access for completed projects, inactive accounts, and file / directory permissions. Such reviews should occur regularly.

Implementation Tip and/or Reasoning

The content transfer system is the computer and networking equipment which accesses the internet for content transfers to and from the production (e.g. dailies). The content transfer system should be the only system enabled to transfer content via the internet.

A minimum number of staff should be given credentials to access the content transfer system to export or import content.

5.6.2 CONTENT TRANSFER SYSTEM GUIDELINES

PROD MGMT SEC TEAM IT

Best Practice

Guidelines for content transfer systems and download machines include, but are not limited to:

- The content transfer system should be used to deliver all digital content
- Only authorized users should have access to the content transfer system
- Access should be restricted on a project basis to individual users who have a business need to use the system
- The content transfer system should be limited to transferring content, streaming content, and key distribution
- 256-bit AES encryption or greater should be used prior to transmission (i.e., encryption at rest) and during transmission (i.e., encryption in transit)
- The web portal / content transfer system should be integrated into a directory service access management system. (See section *5.10 Privileged Access Management & User Accounts*.) If this is not possible, unique credentials should be assigned to each individual user
- The content transfer system should reside on a dedicated server or workstation in the DMZ. Alternatively, it can reside on the segregated portion of the network that does not have access to the source content
- Accounts and passwords for the content transfer system should follow the guidelines listed in the section *5.10 Privileged Access Management & User Accounts*
- An email notification to a designated Security Team member should be sent whenever data is transferred

5.6.3 CONTENT TRANSFER / DATA IO SYSTEMS

IT

Best Practice

Content Transfer services and download machines are required, at a minimum, to conform to the following guidelines:

- Restrictions (e.g., ACLs, firewall rules, or a whitelist of IP addresses) should be configured to disable unrestricted access to the internet from within the Data I/O network
- Data I/O and production networks should be physically separate networks or Virtual LANs (VLANs)
- The Data I/O network should access the internet for the sole purpose of ingest and egress of content
- Internet access for the Data I/O network should be restricted solely to approved file transfer locations
- Data I/O networks cannot initiate connections to internal network segments
- Data I/O machines should be placed in a Restricted Access area monitored, if possible by CCTV.

5.6.4 TRANSFER TOOLS & SERVICES

PROD MGMT SEC TEAM IT

Best Practice

Transfers of content should only occur over secure, encrypted file-transfer platforms. Outbound traffic should be whitelisted to approved service sites only.
See Cloud Services Settings for additional recommendations.

Implementation Tip and/or Reasoning

If available, request Studio Security recommendations or approved vendors.

Do not use any free or consumer grade transfer services.

5.6.5 WEB PORTAL SYSTEMS

IT

Best Practice

Web portal systems should be located on a dedicated server in the DMZ. Access to servers in the DMZ should be restricted by the guidelines defined in paragraph *5.6.1 Content Transfer System Guidelines*.

5.6.6 PORTAL / TRANSFER SYSTEM USERS

IT

Best Practice

Portal user access should be strictly administered. Where available, access should be managed by a directory service access management system. See section *5.10 Privileged Access Management & User Accounts*.

Alternative Approach

At a minimum, users should be assigned unique credentials (i.e., a username and password). See paragraph *5.10.5 Passwords Policy*.

5.6.7 CONTENT ENCRYPTION KEY

IT

Best Practice

Keys used to encrypt content should include an expiration date within a designated period of time. The timeline(s) should align with project / show timelines.

Encryption Key should be provided to content recipient via out-of-band transfer (e.g. separately and by a different method than the encrypted content.) See “Password Policy”.

5.6.8 DATA INGEST ANTI-VIRUS/ANTI-MALWARE/MALICIOUS BEHAVIOUR SCANNING

IT

Best Practice

All data ingested should be scanned by Anti-virus, malware and/or malicious behavior scanning services prior to transfer from Data I/O and ingest into the production environment.

Note: Modern viruses and malware are more and more often designed to evade the signature-based scanning of anti-virus and anti-malware solutions. There are new services which monitor the behavior of files and applications when opened to detect malicious actions.

5.6.9 SECURE DELETION FROM DATA I/O SYSTEM

SEC TEAM IT

Best Practice

Data I/O systems should not be used for digital asset storage. Storage of digital transfers to data I/O machines should be used on a temporary basis for the sole purpose of file ingest and egress. Once the transfer is complete, the content should be securely deleted.

Deletes may be performed manually or through automation. (See paragraph *4.9.2 Destruction of Content*.)

5.7 REMOTE ACCESS TO PRODUCTION NETWORKS

5.7.1 REMOTE ACCESS POLICY

PROD MGMT SEC TEAM IT

Best Practice

Remote Access Settings Policy

Remote access policies, procedures, and systems should be implemented for VPNs into any network or infrastructure device. Guidelines include, but are not limited to:

- Remote access to production networks should be explicitly prohibited unless through Bastion host model. [A Bastion Host is a separate computer on a network specifically designed and configured to withstand attacks.]
- Remote access to production networks should be facilitated through an approved Bastion host model (e.g., Terminal Services) with the ability to move content between sessions restricted.
- Remote access should be linked into central administration systems (e.g., Directory Service, LDAP, and Radius) (See section *5.10 Privileged Access Management & User Accounts*.)
- An audit trail recording the time, date, and activities related to the VPN should be maintained.
- Split tunnel traffic is explicitly prohibited

Remote Access User Policy

Users should have a business case to support remote access and should undergo an approval process prior to being granted access. Guidelines include, but are not limited to:

- Remote access accounts should not be shared
- Remote access should be limited to the fewest people possible
- The remote access user account list should be reviewed regularly. Accounts that are no longer active should be disabled
- Persistent remote access connections should only be permitted for explicitly authorized production processes (e.g., render and transcoding queue management)
- Upon termination, an employee's remote access should be immediately disabled

Implementation Tip and/or Reasoning

Providing remote access extends the production’s digital perimeter. Robust methods to restrict the remote access such as the use of access managers and terminal services are essential.

5.7.2 REMOTE ACCESS – USER AUTHENTICATION

PROD MGMT **IT**

Best Practice

It is recommended that in addition to user authentication via central administration system that two-factor authentication be required for VPN access to production networks. This includes confirming at least two of the following:

- Something the user knows (e.g., a username or password)
- Something the user has (e.g., a token, smartphone, or certificate)
- Something the user is (e.g., biometrics)

Implementation Tip and/or Reasoning

Remote users are unseen. Two-factor authentication is a means to confirm the user is who they say they are and not a hacker impersonating them.

5.7.3 SITE-TO-SITE CONNECTIONS

PROD MGMT **SEC TEAM** **IT**

Best Practice

Site-to-site connections should be supported via a VPN unless connections are dedicated, dark fiber that is point to point or MPLS. Any VPN client or connection should utilize advanced encryption standard (AES) at 256-bits or higher.

5.7.4 REMOTE SYSTEM ADMINISTRATOR / IT SUPPORT ACCESS

IT

Best Practice

In addition to meeting all prior VPN remote access requirements, system administrator remote access should not allow administrative access to network infrastructure for any network or system used to store, transfer, or manipulate content.

Persistent connections are permitted for remote access to service VLAN for IT support and explicitly authorized production access (e.g., render and transcoding queue management)

Access for system outages, troubleshooting, and maintenance is allowed via remote connections that are enabled when needed and disabled immediately after use

The use of a dedicated jump box or remote KVM access should be considered before direct remote access is allowed

5.7.5 THIRD-PARTY REMOTE ACCESS

	PROD MGMT	SEC TEAM	IT

Best Practice

Third-party VPN remote access should only be used in cases where no other solution is available.

All third-party VPN remote access should have a finite end date and be reviewed for activity regularly and disabled if inactive.

Third-party VPN remote access should not provide access to network infrastructure that includes networks or systems used to store, transfer, or manipulate content

All third-party access sessions should be monitored by an employee and logged

Third-party systems used for remote access should be subjected to production inspection to ensure production security policies are enforced.

5.8 USE OF CLOUD SERVICES

5.8.1 SELECTION OF CLOUD SERVICES – SECURITY VETTING

EXEC MGMT	PROD MGMT	SEC TEAM	IT

Best Practice

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

Cloud vendor security services should include but are not limited to:

- Segregated customer data
- SAML 2.0 for single-sign-on user authentication
- Automated user provisioning
- Encrypt customer data in transit and at rest
- Restrict access of service administrators and support technicians to customer data and user information
- User Grouping and User access controls to provide data access privilege limitations
- Audit access and activity logging
- Meet appropriate regulatory security requirements

- Service Level Agreement offering acceptable guarantees of service

Alternative Approach

If any of the above services are not offered, or if answers to the security questionnaire are inadequate, it is highly recommended to use a different cloud service. If for creative purposes there is not an alternative service, address the vendor's security limitations with strict internal alternatives to limit data loss exposure, such as, but not limited to:

- Limit data stored
- Limit service access
- Limit term of use
- Harden internal security measures which may counter the weaknesses of the service provider.

Implementation Tip and/or Reasoning

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.

5.8.2 CLOUD ACCESS SECURITY BROKERS

PROD MGMT **IT**

Best Practice

Use of a cloud access security broker (CASB) for managing user access to cloud services should be implemented with all cloud services that offer LDAP or SAML authentication.

Implementation Tip and/or Reasoning

CASB provide centralized and simplified user management and may be federated to sync users and user groups from the local directory services. (See section *5.10 Privileged Access Management & User Accounts*)

5.8.3 CLOUD SERVICES SETTINGS

PROD MGMT **SEC TEAM** **IT**

Best Practice

Use of cloud services (e.g. applications (SaaS) or platforms (PaaS) accessed via the internet) should adhere to the following guidelines:

SYSTEM REQUIREMENTS

Service access should be authenticated via a CASB single-sign-on identity management provider.

Unique Credentials should be assigned to each user, shared/generic accounts should not be permitted.

If single-sign-on is unavailable, an inventory of users, their application rights assignments and status (active, suspended, de-activated) should be maintained.

URLs to cloud instances should not reference company or show names.

A dedicated instance or domain should be created for each respective production client

Administrative privileges to the instance should be

- restricted to system admins and supervisors or like roles and
- limited to as few individuals as possible

Password requirements to each instance should align with security standards

Where possible, external IP addresses associated with the production workstations should be submitted to the cloud service and whitelisted on their end

NETWORK REQUIREMENTS

The ability to access cloud services should be restricted to machines residing on secure production networks

Outbound internet traffic from the production environment to cloud services should be routed through a proxy (e.g., squid or the like) hosted on a DMZ or like segment.

URLs filtering should be enabled and applied to production workstations which require access to cloud services. Traffic should be restricted to the specified whitelisted URLs.

5.8.4 CLOUD STORAGE / FILE SHARING SERVICES

PROD MGMT **SEC TEAM** **IT**

Best Practice

If cloud file sharing services are used, in addition to the above “Cloud Service Settings”, the following guidelines should be implemented:

- Use Enterprise grade licenses. Do NOT use free or consumer grade licenses.
- Enable single-sign-on authentication
- Access should be restricted to specific folders and sub-folders based on the user’s job role and the principle of least privilege
- Access should be managed by assigning privileges to User Groups and assigning users to the appropriate groups.
- Use Server Sync options and map local server to production workstations to steer content storage to production servers
- Disable user syncing to prevent content being stored locally on user computers and mobile devices

Alternative Approach

If cloud sharing services are used but single-sign-on and / or server sync are unavailable, the following guidelines should be implemented:

- Use Enterprise or Business grade licenses. Do NOT use free or consumer grade licenses.
- Maintain inventory of users, status and access privileges
- Access should be restricted to specific folders and sub-folders based on the user's job role and the principle of least privilege
- Access should be managed by assigning privileges to User Groups and assigning users to the appropriate groups.
- Disable user syncing to prevent content being stored locally on user computers and mobile devices, require users to upload files to the service.
- Or, alternatively, if user device syncing is permitted (*not recommended*): when user is suspended or deactivated, revoke folder and file permissions prior to notifying user to prevent user moving files out of protected folders to local document folders.

Implementation Tip and/or Reasoning

Generally only Enterprise licenses provide access to single-sign-on solution integrations and local server syncing.

5.9 DEVICE SECURITY

5.9.1 SECURING COMPUTER AND MOBILE DEVICES

EXEC MGMT **PROD MGMT** **SEC TEAM** **IT**

Best Practice

Company provided 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.)
All computers within the production network should be hardened. The guidelines include, but are not limited to:

- Up to date operating systems and software
- Up to date software firewall and
- Up to date anti-virus/malware (for Macs as well as PCs) with current DAT files.
- Password protection
- Hard drive encryption - e.g. Mac FileVault or Windows BitLocker

- Removing all unnecessary software
- Disabling all unnecessary services
- Configured with a screensaver. The screensaver should prompt password confirmation upon login, wake-on-sleep, and screensaver. Screensavers should require a password after 10 minutes of idle time.
- Use a wired connection to the production network unless a restricted access production wireless network is in place
- Enable automated backups
- Additionally, for mobile devices (laptops, tablets smartphones) endpoint management protection to:
  - monitor the device settings and alert for device non-compliance with minimum security settings requirements
  - remotely lock or wipe lost or stolen devices
  - remotely enable/disable the camera
  - direct photos to production managed cloud storage, disable personal photo storage solutions (e.g. iCloud, Google Photos, etc.)
  - manage white and blacklisted mobile apps (e.g. social media apps, consumer file sharing apps, etc.)

Alternative Approach

Managed employee owned devices: Bring Your Own "BYOD"s

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. The endpoint manager configuration should verify that each enrolled BYOD has:

- Up to date operating systems and software
- Up to date firewall and anti-virus/malware (for Macs as well as PCs)
- Password protection (at bootup, at awaken, at resume if device is unattended for a set period of time e.g. 3 minutes)
- Hard drive encryption - e.g. Mac FileVault or Windows BitLocker
- Automated backup service of user identified "work product folder"
- Disable user personal automated backup of "work product folder"

Mobile devices (laptops, tablets, smartphones) which access the internet via mobile data services or public Wi-Fi) should have additional protection of Endpoint Management to:

- monitor the device settings and alert for device non-compliance with minimum security settings requirements
- remotely lock or wipe lost or stolen devices
- remotely enable/disable the camera

- direct photos to production managed cloud storage, disable personal photo storage solutions (e.g. iCloud, Google Photos, etc.)

Unsupervised BYODs (NOT RECOMMENDED)

It must be strongly stated, *it is not recommended* to permit unsupervised personal devices (computers, laptops, smartphones, tablets, etc.) to access production networks or data.

In the case production permits the use of unsupervised – "un-trusted" – personal devices within the production perimeters, the following should be required of the device owners:

- Device compliance with production device security guidelines
- Enrollment of devices in personal device protection program which provides remote lock and wipe of lost or stolen devices
- Disabling of automated photo uploads (e.g. iCloud, Google Photos, etc.)
- Enrollment in company automated backup service of user identified "work product folder"
- Disable user personal automated backup of "work product folder"

5.9.2 COMPUTERS STORING CONTENT/CONFIDENTIAL DATA

PROD MGMT SEC TEAM IT

Best Practice

System security for workstations storing content (e.g. Avids, Digital Asset Management workstations, Video Assist or DIT systems) should meet all of the "Securing Computer and Mobile Devices" settings and add additional measures, including but not be limited to:

- Disabling mass storage device driver functionality to ensure that external drives cannot be mounted.
- Disabling USB and other external ports.
- Disabling Internet access unless there is a business requirement that precludes it.
- Implementing physical Ethernet cable locks to ensure that this single network cable cannot be connected to an alternate or unauthorized device. This is especially important if the system is in the same room as other standalone devices, servers, or workstations.
- Tie workstation MAC address to the network port it is connected to.

5.9.3 I/O DEVICES AND DATA TRANSFER PORTS (E.G. USB PORTS)

PROD MGMT SEC TEAM IT

Best Practice

All I/O devices (e.g., USB, FireWire, eSATA, and internal CD / DVD drives) should be disabled or removed from any computer that receives, sends, manipulates, or stores content in the production network. Data transfer ports (e.g. USB ports) should be disabled.

Alternative Approach

Endpoint Management settings for any computer that receives, sends, manipulates, or stores content in the production network should monitor all I/O devices (e.g. USB, portable hard-drives, flash drives, DVD drives) and ports. Data transfer ports (e.g. USB ports) should be disabled.

5.9.4 WORKSTATION/DEVICE GUEST ACCOUNTS

	PROD MGMT	SEC TEAM	IT	

Best Practice

Guest accounts should be disabled or removed from workstations that receive, send, manipulate, or store content in the production network.

Implementation Tip and/or Reasoning

No computers which access production network or digital assets should be shared. If sharing of a computer is necessary, it should only occur between crew who have equal access privileges to information and content.

5.9.5 INTERNET ACCESS LIMITATIONS

	PROD MGMT	SEC TEAM	IT	

Best Practice

Internet access by workstations that receive, send, manipulate, or store confidential data and/or content in the production network should be limited based on workflow requirements. Workstations which do not have specific internet access needs should by default NOT access the internet.

Limiting access to the internet includes endpoint management controls to lock ports which may be used to bypass the network and access the internet via alternative mobile networks (e.g. Mobile hotspots or tethering via USB ports.)

All access to the internet should be limited and monitored (e.g. whitelisted IP addresses, services.)

5.9.6 SECURITY FOR DEVICES ACCESSING THE INTERNET

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

All devices accessing the internet should have at a minimum:

- Up to date operating systems and software
- Up to date firewall and anti-malware (for Macs as well as PCs)

- Password protection (at bootup, at awaken, at resume if device is unattended for a set period of time e.g. 3 minutes)
- Hard drive encryption - e.g. Mac FileVault or Windows BitLocker

Mobile devices (laptops, tablets, smartphones) which access the internet via mobile data services or public Wi-Fi should have additional protections:

Mobile Device Management or Endpoint Management installed to:

- monitor the device settings and alert for device non-compliance with minimum security settings requirements
- remotely lock or wipe lost or stolen devices

Alternative Approach

As part of the production security policies and training, production staff should be trained in the importance of securing all devices that access the internet listed above.

This includes installing production supervised Mobile Device or Endpoint Management.

Implementation Tip and/or Reasoning

Internet access is essential to business functions but it 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 KEYS	SEC TEAM	IT	3RD

Best Practice

Local firewalls should be implemented to restrict access to each workstation. Workstations should have local firewalls implemented to restrict unauthorized access. Please refer to the section *5.2 Firewall and Security Services* for more information.

Implementation Tip and/or Reasoning

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

5.9.8 DEVICE ENCRYPTION

ALL KEYS	SEC TEAM	IT	3RD

Best Practice

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.

Implementation Tip and/or Reasoning

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

5.9.9 SERVER HARDENING

		IT	

Best Practice

Servers should be hardened. Guidelines include, but are not limited to:

- Disabling guest accounts and shares
- Installing antivirus protection
- Enabling software firewalls
- Removing all unnecessary software
- Disabling all unnecessary services
- Requiring all users to operate as restricted users
- Conducting vulnerability scans for hosts that reside in the DMZ every three months at a minimum

5.9.10 IOT AND NETWORK DEVICES (PRINTERS, MULTI-PURPOSE, REMOTE MONITORING, ETC.)

Best Practice

Change all factory setting and/or default user names and passwords.
Limit network access to LAN only. Do not allow internet access unless required for device functionality.
Each IOT device should connect to a single network, no IOT device should service multiple networks.
IOT devices providing general services (e.g. IOT security systems) which do not relate to the creation, modification or storage of data should be segregated from General Production or Restricted Access Networks.

5.10 PRIVILEGED ACCESS MANAGEMENT & USER ACCOUNTS

5.10.1 CENTRAL ADMINISTRATION SYSTEM/DIRECTORY SERVICES

PROD MGMT IT

Best Practice

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. The cloud equivalent: cloud access security brokers (CASB) should be used for authentication to cloud services. CASBs can be federated to the local directory service to sync users and user group assignments. (See paragraph *5.10.3 Access Rights Administration.)*

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.)

Alternative Approach

Unique individual usernames, strong passwords, and / or certificates or biometrics should be required to access any infrastructure, shared storage, server, computer, or laptop device.

Implementation Tip and/or Reasoning

Identity Access Management systems provide central user identity management and verification.

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).

5.10.2 ACCOUNT MANAGEMENT PROCESS

PROD MGMT SEC TEAM IT

Best Practice

An account management process to review administrator, user, and service accounts for systems and applications that store or transfer content should be maintained. This process should include, but not be limited to:

- New user requests
- User access modifications
- Disabling and enabling of user accounts
- User termination
- Account expiration e.g., user accounts should be configured to expire upon the completion of their employment
- Account suspensions for crew temporarily off-production
- Evidence of approvals

5.10.3 ACCESS RIGHTS ADMINISTRATION

EXEC MGMT **PROD MGMT** **SEC TEAM** **IT**

Best Practice

Policies and procedures to govern the administration of access rights should be documented. Guidelines include, but are not limited to:

- Periodic review of the administrator and service accounts to identify unusual, inappropriate, or suspicious behavior and to investigate possible misuse of access privileges
- Establish and periodically review file / directory permissions of key applications such as the content management system, inventory tracking system, accounting and payroll systems to ensure that access is limited to only those who require it
- Grant access rights to User Groups and assign individual users to the user groups appropriate for their role.
- All third-party accounts should be checked upon completion of contract to ensure deactivation.
- Disabling accounts that are inactive
- Maintaining a list of personnel who have admin rights for each system that has access to content
- Restricting the use of administrator or root accounts to applications not compatible with a service account
- Restricting the use of any administrator or root accounts according to principles of least privilege
- Using Authentication, Authorization and Accounting (AAA) for account management for infrastructure devices
- Renaming default administrator accounts and changing passwords for all installed software / hardware (e.g. printers, routers, other hardware - factory admin settings should be changed.)
- Ensuring that all unused administrator accounts are disabled

Implementation Tip and/or Reasoning

"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

	PROD MGMT	SEC TEAM	IT	

Best Practice

Only Trusted Devices - devices registered to the network via directory services and/or enrolled in an Endpoint Management system - should access any infrastructure, shared storage, server, or information/content processing applications.

Macs and Linux computers should be bound to the domain using third-party utilities.

Users should be prohibited from accessing their own workstations as administrators.

Implementation Tip and/or Reasoning

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

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

Policies should be established to enforce the use of unique accounts and passwords for all information systems. Accounts or certificates should not be shared and should be assigned to a specific individual.

A password policy which includes but is not limited to the following, should be implemented:

- Sharing of passwords is prohibited
- Passwords should have a minimum length of eight characters for any account, 12 or more characters is preferred
- Passwords may be phrases or combinations of words and numbers memorable to the user but non-sensical to others as an alternative to passwords which contain three of the following four parameters: upper and lowercase letters, numbers, and special characters
- Unique passwords should be used for each application and/or device - no passwords should be re-used
- The maximum number of invalid login attempts should be between three and five
- Each password should be different from the previous password, with a password history of 10 previous passwords for any account
- Formal procedures should be communicated to all users regarding the proper handling and control of passwords (e.g., never sending a username and password in a single email and refraining from sharing passwords over the phone)

Additional policy for encrypted data:

- Decryption keys and passwords should be delivered via out-of-band transfer (e.g. separately and by a different method than the encrypted data)
- Key names and passwords should never be related to the project or content

Additional policy for data links:

- Usernames and passwords should not be embedded in content links
- User credentials and content links should be distributed via separate emails or SMS texts

Policy and procedures governing management of passwords to user accounts and decryption keys to content should abide to the following guidelines at a minimum:

- Decryption keys and passwords should be delivered via out-of-band transfer (i.e. by separate and different means.)
- Key names and passwords should never be related to the project or content

Alternative Approach

Exceptions for shared user credentials may be necessary for services such as Aspera which ties transfers to a user account and the transfer stops if the user logs out and no other user account can see the progress of that transfer. Sharing of Data I/O user accounts is permissible if different users need to complete the transfer using the system over different shifts. In this case a unique Data I/O computer user identity should be created. No user should share their credentials for any other system. The Data I/O computer should be placed in an access-controlled area and monitored by CCTV. Activity logs should be enabled to allow this exception.

Implementation Tip and/or Reasoning

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

5.10.6 MULTI-FACTOR AUTHENTICATION POLICY

PROD MGMT   SEC TEAM   IT

Best Practice

Policies should be established to identify restricted access resources (e.g. System and Network Administration, Remote Access VPN, Data I/O Server) and require multi-factor authentication for access.

Multi-factor authentication includes confirming at least two of the following:

- Something the user knows (e.g., a username or password)
- Something the user has (e.g., a token, smartphone, or certificate)
- Something the user is (e.g., biometrics)

Implementation Tip and/or Reasoning

Multi-factor authentication should be implemented for access to as many data resources and services as are tolerable. A vast majority of hacks occur via user credential theft and user impersonation. Adding additional authentication steps decreases the threat and increases the perimeter security.

As with good password policy, teaching the value of multi-factor authentication is good for everyone at work and at home.

5.10.7 ACCESS RIGHTS ASSIGNMENTS

PROD MGMT   SEC TEAM   IT

Best Practice

Access Rights or Privileges assignment guidelines include but are not limited to:

- Create access rules based on User Groups
- Assign access to resources and data by User Group (e.g. server and folder access, software license access, cloud service and folder or container access)
- Assign data privileges by User Group (e.g. edit, share, copy, print, annotate, preview only, etc.)
- Assign users to User Groups based on their job role.
- Apply the rule of “least privilege”. Assign the minimum access as required for each User Group and its user members to complete their tasks.

Implementation Tip and/or Reasoning

The use of Directory Services and or Cloud Access Security Brokers can centralize the management of user and user group assignments.

5.10.8 ACCESS TO DATA ON PORTABLE AND LOCAL DEVICES/COMPUTERS

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

Computers, smartphones, tablets and portable hard drives, USB sticks and flash drives should be encrypted and require user authentication to decrypt. Methods of authentication are:

- a digital pin.
- two factor authentication using physical keys or biometric access

All digital pins and physical keys should be provided to the recipient separately from the drive itself

Implementation Tip and/or Reasoning

Supply secure portable devices which offer built-in encryption.

Provide instructions for encrypting smartphones, tablets and computers (Macs: FileVault, PCs: BitLocker).

Do not send the key with the safe. When delivering an encrypted portable drive, use a different delivery method to deliver the key or pin to the drive. E.g. phone or text the recipient to inform them the pin #.

5.11 PATCH / UPDATE MANAGEMENT

5.11.1 PATCH MANAGEMENT

			IT	

Best Practice

A patch management process for all devices (e.g., firewalls, routers, switches, Storage Area Network switches) and systems should be implemented and maintained based on the severity of the threat. The process should include, but not be limited to:

- Outlining exception guidelines for systems / applications that are unable to be patched
- Providing compensating controls for exceptions in which there is a legitimate business case for not patching the system
- Deploying patches deemed “critical” within 72 hours
- Using a centralized patch management tool to automatically deploy the patches.

Alternative Approach

Networks, systems and/or devices which are incompatible with current operating systems or patches should be segregated from all others and, if possible, from the internet.

Implementation Tip and/or Reasoning

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

5.11.2 CHANGE MANAGEMENT

ALL KEYS	SEC TEAM	IT	3RD

Best Practice

All devices connected to production networks should be maintained with current operating systems and application security patches with the exception that such an application is incompatible with an upgrade.

A change management process for all infrastructure and technology should be implemented and maintained to address precautions and steps to be taken when deciding to and implementing equipment changes, software upgrades, software and operating system updates. This process should include, but not be limited to:

- Reviewing and approving any scheduled changes prior to their implementation
- Maintaining a record of approved and implemented changes
- Reviewing security controls and integrity procedures to ensure they will not be compromised by changes
- Ensuring that appropriate backup or roll-back procedures are documented and tested
- Identifying all affected computer software, data files, database entities, and infrastructure
- Minimizing business disruption when implementing change
- Maintaining an audit log of all change requests
- Maintaining a version control for all software changes

Alternative Approach

Policy for employee owned “bring-your-own-devices” BYODs should include the requirement to maintain the most current versions of the operating system and all installed applications. Use of Auto-Update is recommended except in particular circumstances of application incompatibility.

Implementation Tip and/or Reasoning

In today’s world of new viruses, malware and attack vectors invented daily, it is critical to keep all operating systems and applications updated to their most current release. 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

5.12.1 DATA BACKUP STRATEGY

EXEC MGMT	**PROD MGMT**	**SEC TEAM**	**IT**

Best Practice

It is important to establish backup policies to address the many potential risks to data and how the backups may serve to mitigate those risks (e.g. erroneous deletions, equipment damages, loss or theft, criminal data ransoming or data destruction.)
Items to consider include, but are not limited to:

- Frequency of backup and reconciliation of device and systems efficiency versus periods of exposure for lack of backup copies.
- Number of versions of altered files retained reconciled with the amount of storage required.
- Period of time backups and file versions are retained reconciled with the amount of storage and the exposure to ransomware attacks.
- Policy regarding "Backup" for quick and easy restoration versus "Archive" for long term storage and rare restoration.
- Period of time allowed until data is converted from "Backup" to "Archive".
- Frequency of full backups versus incremental backups of changes only and differential backups for specified time periods (e.g. continuous incremental, weekly differential, and monthly full backups.) And, frequency the incremental and differential backups are securely deleted.

Implementation Tip and/or Reasoning

The better thought out the backup strategy, the more effective it will be when the need to restore arises. Train those staff using their own BYOD devices on the backup strategy and require them to implement an equal backup plan.

5.12.2 DATA BACKUP

EXEC MGMT	**ALL KEYS**	**SEC TEAM**	**IT**	**3RD**

Best Practice

All devices should be backed up continuously or incrementally daily to capture and secure work in progress. Additional backup guidelines include, but are not limited to:

- Backup data stored in a secure, offsite location should be encrypted using AES with at least 256-bit key strength
- Policies and procedures should be in place to allow prompt recovery of data

- Policies and procedures should be in place to determine the number of file versions and the period of time retained in backup.
- Backup solution should be regularly tested to confirm that it restores data successfully
- Review process should be in place to ensure that only authorized administrators are able to access backup location

Implementation Tip and/or Reasoning

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

5.12.3 BACK UP COPIES

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

Guidelines on backup copies include but are not limited to:

- Backup copies of content onto a portable device (e.g., a portable hard drive or USB stick) should use the same security controls applied to the original versions, i.e., all copies and versions of content should be equally protected. Backup portable devices should be encrypted – see paragraph 5.9.8 Device Encryption.
- If the backup system uses administrator credentials to connect to a system, it should not be shared with any other system
- Tape backups (e.g. LTO tapes) should be secured in locked storage onsite, if stored offsite, tape backups should be encrypted
- The reuse of physical media (e.g., LTO tape) should only occur after full erasure of the prior data. It is recommended to use one-pass overwriting that meets NIST Media Sanitization Standards SP 800-88

5.12.4 BACK UP OF PERSONAL DEVICES

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

Follow the Data Backup guidelines.

Identify appropriate file folder(s) to backup to company managed backup and archive services (i.e. device owner should identify specific folder where all production work product will be stored and where no personal files or data will be stored.)

User’s personal automated backup should EXCLUDE the above identified file folder(s).

5.13 VULNERABILITY ASSESSMENT AND PENETRATION TESTING

5.13.1 PENETRATION TESTING

PROD MGMT SEC TEAM IT

Best Practice

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.

If a third-party IT provider is used to provide network administration services, a different provider should be used for penetration testing. Critical security issues should be remediated in accordance with the Production's Security Policy.

A penetration test should involve a Red Team (attacker) and a Blue Team (defender). The Red and Blue teams may be separate contractors or a contractor and the production IT team.

Alternative Approach

If available, ask Studio IT or Security to check the installation.

Implementation Tip and/or Reasoning

Purple Team exercises may provide valuable feedback and consultation between the Red and Blue during the testing.

Do not assume the trustworthiness, nor the security expertise of third-party IT services providers. Check references, particularly from IT security professionals. Check credentials and 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.

5.13.2 TESTING POLICY

PROD MGMT IT

Best Practice

Productions, established for over 12 months at any one facility, should have a policy for performing digital security vulnerability / risk assessments / penetration (PEN) tests of external IP ranges, hosts and internal networks annually.

Personnel conducting tests should provide a summary of the test results and include signoff from those who performed the test and those who reviewed the results.

Critical issues identified that provide unauthorized access to productions systems and content should be remediated according to the policy.

5.13.3 VULNERABILITY SCANS

PROD MGMT **IT**

Best Practice

Vulnerability scans of all external IP ranges and hosts should be performed at least every three months.

Internal network vulnerability scans should be performed upon completion of setup and at least annually if installation is long term.

Findings, results, and remediation activities should all be documented and readily available for review.

Implementation Tip and/or Reasoning

Engage 3rd party who has not installed nor maintained network(s).

5.14 SYSTEMS AND SECURITY MONITORING & LOGGING

5.14.1 SYSTEM LOGGING

PROD MGMT **IT**

Best Practice

Productions should implement policies and procedures for system logging on all network and system devices. This includes production operating systems, content management components, and systems with internet access. These devices include:

- Firewalls
- Authentication servers and network operating systems
- Production operating systems
- Content management devices (i.e., all network devices, storage devices, content servers, and content storage tools)

- Systems with internet access
- VPN Access

System Logging requirements should include, but are not limited to:

- Retaining logs for duration of production
- Restricting the list of administrators or auditors with access to logs based on business needs
- Frequently scheduled reviews of audit logs for unusual activity
- Isolating and securing log data (e.g., log aggregation and encryption) to a central server
- Preventing unauthorized access or modification of log data
- Using a dedicated server to manage the logs in a central repository with a syslog or log-management server, security information, and event management tool

Use a system logging tool to collect and aggregate searchable data logs and to identify suspicious activities for automated alerts.

Implementation Tip and/or Reasoning

At a minimum, set up monitoring and logging for the network segment(s) containing the most valuable data assets: Content.

5.14.2 MONITORING CONTROLS SETTINGS

IT

Best Practice

Logging monitoring controls should be set to log system and application activity, exceptions, security-related events, and actions across all systems. The monitoring controls should be configured to include but not be limited to:

- Logging and reporting in real-time
- Time stamping
- Source / location information
- Usernames
- Context of use
- Netflow logs summary

5.14.3 AUTOMATIC NOTIFICATIONS

PROD MGMT **SEC TEAM** **IT**

Best Practice

A list of events that require automatic notification to the appropriate Security Team member(s) for investigation should be defined. Automated alerts should be configured to notify appropriate personnel based on conditions that include, but are not limited to:

- Successful / unsuccessful attempts to connect to the content or production network
- Unusual file size or time-of-day transport of content
- Repeated attempts for unauthorized file access
- Attempts to secure privilege elevation

Implementation Tip and/or Reasoning

Designated Security Team member should be trained to understand the notifications, their severity and urgency to investigate and mitigate.

It is important that settings do not trigger so many alerts that a “boy who cried wolf” syndrome develops. If excessive false-alerts are generated, review and adjust the settings.

Notifications should not be the sole trigger to review the monitor logs. Logs should be reviewed regularly for suspicious activities which may have been missed in the automatic notifications settings.

(RETURN TO TABLE OF CONTENTS)

VI. PLANNING FOR SECURITY & RESPONSE TO BREACHES

6.1 PLANNING MANAGEMENT AND WORKFLOWS

6.1.1 SECURITY RISK ASSESSMENTS

EXEC MGMT	ALL KEYS	SEC TEAM	IT	3RD

Best Practice

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:

- creation and/or acquisition of all asset types
- on-set capture and duplication;
- transfer from set to post and to third party facilities;
- sharing and collaboration with creative stakeholders;
- sharing and collaboration with financiers, partners, vendors, representatives, etc.;
- transfers between personnel and between facilities.

Assessments should address:

- Various site outage scenarios due to natural or non-natural disasters, including prolonged failure of technical dependencies (e.g., telecommunications, power, transport, etc.)
- Unintentional or malicious modification of content, regulated or confidential information.
- Leak or theft of content, regulated or confidential information.

Implementation Tip and/or Reasoning

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.

A Security Risk Assessment is a review of the planned workflow to identify each point of potential exposure to technical failures, human errors, malicious behaviors, and natural disasters in order to:

- Be aware of vulnerabilities
- Make changes to the workflow to reduce the number and or exposure from vulnerabilities
- Make backup plans to mitigate damages when an adverse event occurs.

Make sure that every step of the process is well mapped out before beginning the process.

Identify each hand-off between steps in the workflow (e.g. set to editorial, payroll to payroll service), between personnel (e.g. assistant editor to editor, producer to talent agent) and between facilities (e.g. editorial to sound house). Review the protocols for each hand-off: who, how, when, where, why.

Create a plan to address breakdowns (e.g. power outage, computer failure, server failure, vehicle breakdown, personnel termination, facility termination, etc.)

6.1.2 BUSINESS CONTINUITY MANAGEMENT (BACKUP PLANNING)

PROD MGMT SEC TEAM IT

Best Practice

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

The Business Continuity Plan should

- provide guidelines for preparedness to use alternative workflows and/or report appropriately when a disruption to their workflows occurs, in particular a disruption which results in delay, damage, destruction or loss of production assets (time, physical, intellectual or digital.)
- address both physical locations and data processing locations (e.g. computers, mobile devices, networks, cloud services)
- be shared with department heads as appropriate to their production roles.
- address reliance on any third parties
- be reviewed and updated
  - whenever a change to the production workflow or locations occurs
  - whenever a disruption has occurred and the continuity plan implemented might be improved

Alternative Approach

Business Continuity Plans may be broken into smaller lists of recommendations appropriate to production workflows and locations considered critical in protecting key production assets, such as media, scripts, and HR records.

Implementation Tip and/or Reasoning

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.

Guidelines of a business continuity plan include but are not limited to:

- Identify the different risk environments and the degree of risk mitigation necessary to protect against losses in the event that disruptions occur
- Training of personnel in regard to their roles in the security of the production
- Identify backup methods and alternative means of communication or transport

6.1.3 INCIDENT REVIEW

PROD MGMT SEC TEAM IT

Best Practice

Following a security breach and its immediate response, an incident review should occur to

- identify perimeter and security measure weaknesses which should be corrected
- identify procedures which need modification
- update security measures, policies and training to incorporate what is learned from the incident review

Implementation Tip and/or Reasoning

Look at specifics of the breach, who, how, what, where, when and identify the scope of the weakness that permitted the breach to occur. Is it specific to a single person or could several individuals with similar access have caused it? Is it specific to a particular location or could several similar locations allow it? Etc.

Then focus on the security measures which did not succeed and revise them, as is feasible, to prevent recurrence. Or, if the weakness is built in (e.g. a location cannot be altered), heighten other measures to compensate (e.g. add security guard.)

6.2 LOG REVIEWS

6.2.1 ACCESS LOGS

PROD MGMT **SEC TEAM**

Best Practice

The production should keep and retain access logs for physical and data access.

Logs should be regularly reviewed for system access needs and abnormal behavior.

Implementation Tip and/or Reasoning

Regular reviews of logs will inform Security Team of normal production behaviors and patterns and make identifying abnormal behaviors more easily identifiable.

Frequent reviews may also reduce damages in case a breach has occurred without provoking an automated alert by reducing the amount of time it goes undetected.

6.3 RESPONDING TO BREACHES

6.3.1 ANONYMOUS REPORTING

EXEC MGMT **PROD MGMT** **SEC TEAM**

Best Practice

Anonymous reporting should be made available to production crew and contractors for reporting of content protection and piracy concerns. The anonymous reporting tool consisting of an internal, anonymous telephone number, email address, and / or website should be published and also provided during security awareness training.

Implementation Tip and/or Reasoning

The anonymous reporting contact for security concerns can be the same as for harassment, health & safety concerns provided clear next steps are outlined to address the receipt of a security concern or breach report.

6.3.2 INCIDENT RESPONSE

EXEC MGMT **PROD MGMT** **SEC TEAM**

Best Practice

In the event that assets are compromised, lost, or stolen, the producer, and if applicable the studio and/or financier(s) should be alerted via a pre-agreed notification chain and method.

Law enforcement should be notified by producer when incidents involving potentially illegal cyber or physical theft occur

Implementation Tip and/or Reasoning

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 12/1/18: The law enforcement office in Los Angeles to contact regarding cybercrime is the Office of the District Attorney - Deputy D.A. Warren Kato: wkato@da.lacounty.gov; +1-213-257-2440.

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

(RETURN TO TABLE OF CONTENTS)