Film & TV Production Security Guidelines

Appendix C – Individual Responsibility

Developed and Maintained by CDSA's
Production Security Working Group

www.CDSAonline.org

INTRODUCTION

AUTHORS

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

PURPOSE

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

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

This appendix outlining the individual's responsibilities may be adapted as a hand-out for individuals or for incorporation into employment or services contracts.

TARGET AUDIENCE

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

This extract of "Individual Responsibilities" summarizes the production security responsibilities of all individuals involved on a production who access, manage, transport or transfer the production's assets.

DEFINITIONS

ASSETS

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

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

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

examples of data asset formats being:

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

Physical Asset: Asset that exist in the physical realm, examples being:

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

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

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

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

- All products of work-for-hire contracts
- Pitch, if purchased
- Treatment
- Synopsis
- Bible
- Scripts
- Casting lists
- Designs
- Concept art
- Research
- Samples
- Costumes and Props manufactured by production
- Sets and Set Decorations manufactured by production
- Unique tools developed and/or manufactured by production
- Versions in progress
- Continuity photos
- Rehearsal photos or footage
- Sound recordings
- Sound samples
- Image recordings
- Edited selections
- Edited cuts
- Un-composited picture or sound layers
- Composited picture or sound layers
- Rejected versions of all the above
- Out-takes
- Unused footage or sound
- And: the release version of the Content

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

- Personally Identifying Information ("**PII**") are any pieces of information that can be combined to identify a unique individual, examples being:
  - name,
  - address,
  - tax or government ID number,
  - phone number,
  - email address,
  - IP address,

- Physical location
- GPS location,
- photo,
- family member

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

Examples of documents which include PII are:

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

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

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

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

HACK

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

HACKER

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

There are many types of hackers:

- Not a User – see "User" below
- Felons – actively seek to hack

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

LEAST PRIVILEGE PRINCIPLE

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

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

NETWORK

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

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

PERIMETER

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

SECURITY TITLE

Pseudonymized title used to maintain secrecy of project in production. Also called Temporary or Working Title 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.

INDIVIDUAL RESPONSIBILITY

All individuals should 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, notify department head or IT to correct the access permission.
- Keeping all devices (computers, smartphones, tablets, etc.) secure with:
    - up to date versions of operating system, browsers and applications. (Most updates today are issued to patch security vulnerabilities, not updating a device turns it into a hacker target.)
    - encrypted (password protected)

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

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