Film & TV Production Security Guidelines

Appendix A: One-Page Security Checklist

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 offers a very high-level checklist for general security awareness.

TARGET AUDIENCE

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

This checklist is designed for **executives** and **managers** who need to be aware of the many requirements to work securely but will not be directly involved with planning, budgeting or implementing the policies.

ONE-PAGE SECURITY CHECKLIST

- **Security starts and ends with people.**
  - ❑ Vet them – references, background checks
  - ❑ Train them – explain, train, hand-outs, posters
  - ❑ Engage them –NDAs and policy compliance
  - ❑ Identify them – ID badges, user IDs
  - ❑ Define roles, assign to groups, grant privileges
  - ❑ Protect them – create a safe workplace, secure their devices, provide a means to report concerns, breaches, and observations.

- **Define assets aka "content" to protect**
  - ❑ Define Work Product
  - ❑ Define Intellectual Property
  - ❑ Define Regulated Information
  - ❑ Define Confidential Information
  - ❑ Define Physical and Digital

- **Define perimeter (where what is controlled & what isn't)**
  - ❑ Secure controlled entries – front door, emergency exits,
  - ❑ windows, gates, loading docks
  - ❑ Secure uncontrolled entries – unfenced base-camp or filming location
  - ❑ Secure/restrict device connectivity and ports such as Ethernet, Wi-Fi, Mobile Networks, USB, Bluetooth, …
  - ❑ Secure network routers, switches, ports
  - ❑ Assess internet provider
  - ❑ Secure/restrict access to vetted Cloud Services
  - ❑ Elect secure communications services: Email, Chat, and Text

- **Defend perimeter**
  - ❑ Identify intruders – no ID badges, fake user IDs
  - ❑ Enforce use of keys, keycards, automatic locks, safes
  - ❑ Install and regularly test alarms and bright lighting
  - ❑ Check locks, change locks after a key is lost or stolen
  - ❑ Isolate restricted, more protected areas – add barriers, CCTV monitoring
  - ❑ Implement user identity and access management service for single-sign-on
  - ❑ Implement user passwords, multi-factor authentication
  - ❑ Implement encryption of devices, communications and content
  - ❑ Deploy endpoint and mobile device management
  - ❑ Close unused device ports and network switches/ports
  - ❑ Deploy firewalls, anti-virus, anti-malware
  - ❑ Segregate networks, assets and access
  - ❑ Backup and archive data

- **Apply policy of "Least Privilege"**
  - ❑ Grant minimum access necessary for each individual to perform job tasks
  - ❑ Limit access to stages, creative offices, editorial
  - ❑ Limit access to services and applications
  - ❑ Limit access to storage
  - ❑ Limit access and actions to shared data storage folders and files
  - ❑ Limit access to the internet

- **Trust but verify**
  - ❑ Request ID badges be worn visibly at all times
  - ❑ Escort visitors at all times
  - ❑ Perform penetration test of networks and systems
  - ❑ Audit or check TPN status of vendors

- **Monitor**
  - ❑ Deploy security guards
  - ❑ Implement reception check-in/check-out
  - ❑ Implement inventory tracking
  - ❑ Implement data system access logging and unusual behavior alerting

- **Document**
  - ❑ Maintain inventories for physical and data assets
  - ❑ Maintain entry-exit logs
  - ❑ Maintain shipping & courier logs
  - ❑ Maintain data system access logs
  - ❑ Maintain data transfer logs
  - ❑ Retain CCTV recordings

- **Plan – review – mitigate – prepare**
  - ❑ Determine role-based access privileges
  - ❑ Plan storage, retention and destruction of assets
  - ❑ Plan workflow and workflow adjustments in case of disruption
  - ❑ Plan response for breach, loss, theft, employee termination
  - ❑ Plan who, when, why and how for reporting of and addressing concerns, incidents and terminations
  - ❑ Review logs regularly and when alerted for unusual behavior
  - ❑ Following an incident: review plan, workflow, setup and revise or mitigate to address discovered weakness

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