MOTION PICTURE ASSOCIATION

MPA Best Practice Guidelines to Consider for Remote Content Handling

Introduction

With the recent COVID-19 pandemic, some post production vendors may be forced to implement remote work solutions, otherwise known as work from home (WFH) to continue operations. This document serves to provide vendors with guidance on which MPA Best Practice Common Guidelines may be considered while working remotely, as part of their Business Continuity Plan (BCP). **Note:** This document is only intended to provide references to existing Best Practices that may be leveraged, and vendors should not infer or conclude that this document replaces content security guidance received directly from content owners. When in doubt vendors should always seek guidance directly from content owners. The MPA does not endorse work from home solutions and vendors must always get approval from content owners prior to implementing any WFH solution. For a copy the MPA Best Practice Common Guidelines referenced in this document refer to the following weblink: https://www.motionpictures.org/best-practices. Vendors are encouraged to reference the Best Practices document for more detailed guidance and additional Best Practices not included here.

Management System

There are several Management System Best Practices that could be leveraged as part WFH scenarios. Below are areas that may be applied prior to and during WFH. These areas include security awareness training, incident response, business continuity planning, and confidentiality/non-disclosure.

- MS-4.3 Develop and regularly update an awareness program about security policies and procedures and train company personnel and third-party workers upon hire and annually thereafter on those security policies and procedures, addressing the following areas at a minimum:
    - IT security policies and procedures
    - Content/asset security and handling in general and client-specific requirements
    - Social media policies
    - Social engineering prevention
    - Security incident reporting and escalation
    - Disciplinary policy
    - Encryption and key management for all individuals who handle encrypted content
    - Asset disposal and destruction processes
    - Ransomware

Last Published 11/11/2020

MPA Best Practice Guidelines to Consider for Remote Content Handling

- MS-5.0 Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported.
- MS-6.0 Establish a formal plan that describes actions to be taken to ensure business continuity
  Consider including the following sections in the business continuity plan:
  - Threats to critical assets and content, including loss of power and telecommunications, systems failure, natural disasters, pandemics, ransomware, etc.
  - Consider cyber security insurance (optional) to help mitigate risks from a cyberattack including, but not limited to: (1) identity theft; (2) business interruption; (3) damage to reputation; (4) data repair costs; (5) theft of customer lists or trade secrets; (6) hardware and software repair costs; (7) credit monitoring services for impacted consumers; and (8) litigation costs
  - A temporary Work From Home (WFH) as an exception process may be considered in situations where working from the office or an alternate work site is not an option. WFH options always require the approval of content owners prior to implementing. Refer to "MPA Best Practice Guidelines to Consider for Remote Content Handling" at the weblink here: https://www.motionpictures.org/best-practices-remote-content-handling for information on which MPA Best Practices may be considered during WFH.
  - Detailed information system, content and metadata backup procedures and information system documentation, including configuration of critical WAN and LAN / Internal Network devices
  - Encryption of backups (AES-256)
  - Backup power supply to support at least 15 minutes for the surveillance camera system, alarm and critical information systems, including software to perform a safe shutdown of critical systems
  - Consider use of an off-site backup location
  - Notification of security team
  - Escalation to management
  - Analysis of impact and priority
  - Containment of impact
  - Priorities for recovery and detailed recovery procedures, including manual workarounds and configuration details of restored systems
  - Key contact information
  - Notification of affected business partners and clients
  - Testing of business continuity and disaster recovery processes at least annually
  - For policy templates example for Disaster Recovery, and Pandemic Response Planning see SANS: https://www.sans.org/information-security-policy/
- MS-11.0 Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and review annually thereafter, that includes requirements for handling and protecting content.

MPA Best Practice Guidelines to Consider for Remote Content Handling

Physical Security

Physical Security Best Practices may be leveraged as part WFH scenarios. Below are areas that may be considered prior to WFH, which include securing the entrances/exits of the remote location, segregating areas that handle content, installing an alarm, and implementing a surveillance camera system.

- PS-1.0 Secure all entry/exit points of the facility at all times, including loading dock doors and windows.
- PS-1.1 Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering).
- PS-5.0 Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.)
- PS-9.0 Install a surveillance camera system (analog CCTV or IP cameras) that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.)

Digital Security

Digital Security Best Practices may also be leveraged as part WFH scenarios. Below are areas that may be considered prior to WFH, which include separating external WAN networks from internal networks using a firewall, prohibiting internet access, email and web filtering, and other areas mentioned below.

- DS-1.0 Separate external network(s)/WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic
- DS-1.6 Do not allow direct management of the firewall from any external interfaces (i.e. Internet or WAN facing)
- DS-2.0 Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session
- DS-2.1 Implement email filtering software or appliances that block the following from non-production networks:
  - Potential phishing emails
  - Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)
  - File size restrictions limited to 30 MB
  - Known domains that are sources of malware or viruses

MPA Best Practice Guidelines to Consider for Remote Content Handling

- DS-2.2 Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites
- DS-3.0 Isolate the content / production network from nonproduction networks (e.g., office network, DMZ, the internet etc.) by means of physical or logical network segmentation
- DS-3.8 Harden systems prior to placing them in the LAN / Internal Network
- DS-4.0 Prohibit wireless networking and the use of wireless devices on the content / production network.
- DS-4.1 Configure non-production wireless networks (e.g., administrative and guest) with the following security controls:
  - Disable WEP / WPA
  - Enable WPA2-PSK (AES)
  - Segregate "guest" networks from the company's other networks
  - Change default administrator logon credentials
  - Change default network name (SSID)
- DS-5.0 Designate specific data I/O systems to be used for uploading / downloading content from / to external networks (Internet).
- DS-6.0 Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems
- DS-6.1 Update all anti-virus and anti-malware definitions daily, or more frequently
- DS-6.2.1 Local firewalls should be implemented on workstations to restrict unauthorized access to the workstation
- DS-6.4 Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/updates that remediate security vulnerabilities
- DS-6.7 Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/mobile devices that handle content to allow remote wiping of hard drives and other storage devices
- DS-7.2 Assign unique credentials on a need-to-know basis using the principles of least privilege
- DS-7.3 Rename the default administrator accounts and other default accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates)

MPA Best Practice Guidelines to Consider for Remote Content Handling

- DS-8.1 Enforce a strong password policy for gaining access to information systems. Password policy should include guidance for service accounts. A facility should opt to choose one or more of the following password policies (Note: additional password policy options are available in the Best Practices document mentioned on page 1):
    - Utilize multi-factor authentication (MFA) that uses a combination of two or more the following:
        - Something they know and only they know (e.g. password)
        - Something they have and only they have (e.g. soft or hard token)
        - Something they and only they are (e.g. biometrics)
    - Create a password policy that consists of the following:
        - Minimum password length of 12 characters
        - Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters
        - Maximum password age of 365 days 4. Minimum password age of 1 day 5. Maximum invalid logon attempts of between 3 and 5 attempts
        - User accounts locked after invalid logon attempts must be manually unlocked, and should not automatically unlock after a certain amount of time has passed
        - Password history of ten previous passwords
- DS-8.2 For remote access (e.g., VPN) to the networks, implement two-factor authentication (e.g., username / password and hard token) and monitor activity
- DS-8.3 Implement password-protected screensavers or screen-lock software for servers and workstations
- DS-11.1 Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES-256 encryption by either:
  • File-based encryption: (i.e., encrypting the content itself)
  • Drive-based encryption: (i.e., encrypting the hard drive)
- DS-12.3 Use client AKAs (“aliases”) in asset tracking systems, unless otherwise as directed by the client
- DS-12.4 Use enterprise (not personal) versions of online or web based collaboration services (e.g., Google Docs, etc.) for tracking content, managing inventory, or workflow management, Utilize multi-factor authentication and centrally managed user accounts and access to data.
- DS-13.0 Use only client-approved transfer systems that utilize access controls, a minimum of AES-256 encryption for content at rest and for content in motion and use strong authentication for content transfer sessions
- DS-14.3 Remove content from content transfer devices/systems immediately after successful transmission/receipt

Other Helpful WFH References:

1. "SANS Security Awareness Work-from-Home Deployment Kit." *SANS Security Awareness*, 2020, www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit.
2. "NIST Cybersecurity Recommendations for Working from Home." *Security Magazine RSS*, Security Magazine, 25 Mar. 2020, www.securitymagazine.com/articles/91990-nist-cybersecurity-recommendations-for-working-from-home.
3. Villanueva, Lisa, and Dustin Brewer. "Managing Remote Work Environments With COBIT 2019." *ISACA COBIT Focus*, 30 Mar. 2020, www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2020/managing-remote-work-environments-with-cobit-2019.

MPA Best Practice Guidelines to Consider for Remote Content Handling

Update Notes:

1. 7.10.20 – First published
2. 8.11.20 – Spelling corrections made on page 1 and 3, added Update Notes section, on page 7
3. 11.6.20 – MS-6.0 was updated to reflect changes in V4.08 of the MPA Best Practices Common Guidelines, D S-8.2 control reference corrected on page 5