AMAZON STUDIOS CONTENT SECURITY

Dailies & Editorial Procedure v2.2

Disclaimer:
It is the responsibility of all personnel, including management, crew members, and contractors to bring instances of non-compliance to the attention of Content-Security@amazon.com. Non-compliance with these policies can result in consequences including, but not limited to, termination and subsequent legal action.

1. Secure Content Handling

Please follow the information below to ensure your content handling workflow aligns with Amazon Studios Content Security standard.

Security Awareness & NDA:

- All content handling staff must review and accept project NDAs
- Complete Content Security Training

Secure Devices & Networks:

- All content handling and transferring/shuttling devices including backup storage must be encrypted (AES-256 or higher)
  - An exception can be granted for DIT cart if on-set physical security is set up sufficiently per Production Security team
- All content handling devices/workstations/storage must be hardened (refer to hyperlink)
- Editing workstations and storages must be physically air-gapped or logically segregated with route restrictions. A dedicated transfer workstation must be set up. See Network Segmentation Guidelines for further information on segmentation and content transfer

Secure Content Flow:

- Ensure that content transfer and sharing are digitally documented and approved by Amazon Post contact prior to the transfer or sharing
  - For physical transfer, do not leave drive/equipment unattended and document chain of custody (e.g. email each drive hand-off with time and date stamp)
- Document the dailies and editorial process (on prem vs. remote) along with raw camera footage handling and transfer process. Upload your diagram here. Please name the diagram with the [code name] + [date mm-dd-yyyy] (e.g. TEST 12-12-2022).
  - See this Example Workflow for reference

Secure 3rd Party and Tooling:

- All 3rd party vendor facilities (AV post, ADR, etc.) and tooling (e.g. BOX, Moxion, PIX, etc.) must be vetted and cleared by Amazon Content Security. Confirm the 3rd party facilities/tooling's security clearance status with Amazon Post contact.

2. Incident Response

If any breach or leak is detected, immediately contact Content-Security@amazon.com with the following information: (a) code name of project, (b) facility detail, (c) contact info, (d) description of the incident, (e) any remediation/mitigation steps taken