amazonstudios
CONTENT
SECURITY

AMAZON STUDIOS CONTENT SECURITY

5 KEY PRINCIPLES TO SECURE AMAZON ORIGINALS

Amazon Studios is committed to providing a secure working environment for the protection of all cast, crew, employees, guests, intellectual property, and our brand. Security relies on the collaborative efforts of all cast and crew members to help proactively mitigate any security issues or incidents. Amazon Studios Content Security needs your help to protect all elements of Amazon Originals! Know the Content Security Principles and familiarize yourself with the **CS Policies** to protect your great works of art!

PRINCIPLE #1

BE SELECTIVE, WORK WITH SECURITY SAVVY VENDORS

START Secured, Trusted And Reviewed Third-Party Assessments

Follow Amazon's security guidelines and best practices at the outset of any project. In many instances, Content Security may also need to conduct a security risk assessment (SRA). Access the START system for a list of approved vendors or to request a secure and trusted, third party assessment.

START
SECURED, TRUSTED AND REVIEWED, THIRD-PARTY ASSESSMENT

☑ All vendors who **access, collect, process, transmit** or store Amazon pre-release content must be **properly on-boarded** by Amazon Studios Content Security. When working with external agencies such as social media, marketing agencies, photographer/videographers, and publicists, be sure to comply with the **Marketing, PR and Promotional Policy.**

Always ensure vendors have signed an NDA, undergone a security assessment, and are approved by Content Security before you share any assets or pre-release content.

☑ Inform Content Security **content-security@amazon.com** if you are planning to use a current vendor in a new way (giving new or different data, etc.) as this may change the level of risk.

PRINCIPLE #2

BEWARE WHAT YOU SHARE!

In today's social media environment, sensitive information is easier to leak than ever before. As tempting as it may be to show the world your work, remember posts can easily go viral, which is why it is imparative to keep sensitive information and materials confidential.

🚫 Never post Amazon Original pre-release content to social media without expressed permission.

Business social media accounts should utilize unique login credentials which should not be shared. Account users and approvers should be tracked in a central registry that does not store passwords in accordance with **Amazon Studios' Social Media Guideline.**

🔒 Passwords must be different for each social media platform/site and contain at least eight characters with a combination of upper/lower case, numeric, and special characters.

Social media sites should only be accessed using Amazon-owned devices.

PRINCIPLE #3

PROTECT AMAZON ORIGINALS DURING PRE-RELEASE AND SCREENINGS

When handling physical hard drives, tapes, or discs for screenings or final delivery, remember to always use non-descriptive packaging and follow encryption procedures to secure content for delivery.

☑ **Studio executive approval is required** for any screener codes given out at awards, festivals, consumer events, and/or market research events.

</> All screener codes sent to advanced screening attendees must be attributable single-use and traceable to approved individuals.

✉ A Digital Cinema Package (DCP) is required for pre-release screenings – please reach out to **Content-Security@amazon.com** for special approval of any non-DCP format for screeners.

PRINCIPLE #4

YOU CAN'T UNSEND CONTENT! HANDLE AMAZON ORIGINAL DATA WITH CARE.

✉ Only use **approved tools** such as Amazon WorkDocs, Amazon Studios instance of Box, and Scenechronize when sending, sharing and storing content. If you're new to the team, **request access to Amazon Studios Box** to begin collaborating securely with colleagues.

Never send pre-release Amazon Original content over regular email and follow the **Asset Handling Standard** to ensure proper storage, transport and destruction of all Amazon Original content.

PRINCIPLE #5

KEEP CONTENT SECURE FROM CONCEPT TO PRIME!

☑ Ensure that all finishing efforts are done in accordance with Amazon Studios **Post-Production Procedures.** When requesting final features, DVDs and Blue-Ray discs, submit a **Content Access Request Form (CARF)** to Post-Ops AND approved authorized approvers to initiate the asset request process.

Assets are tiered by level of security measures required throughout the production life-cycle. Please reach out to **Content-Security@amazon.com** for inquiries on asset tiering.

THINK SECURITY!

KNOW WHERE TO GO FOR HELP!

Check out the Content Security Wiki for more on security services, policies, guidelines, and awareness materials.

Everyone working on an Amazon Original is expected to notify Amazon Studios Content Security at the earliest possible opportunity of any security incidents, including lost or stolen devices that belong to, access, or stores Amazon Studios content.

If you see something you believe could compromise the confidentiality of an Amazon Original, immediately alert **Content Security** content-security@amazon.com

For 24-hour response contact the Amazon Intelligence Security Alert and Awareness Center (ISAAC) Hotline: (206) 800 0547, isaac@amazon.com.

Please include your telephone number and a team member will call you as soon as possible.

Please note that security standards and procedures are subject to change based on technology developments and threats.