SOCIAL MEDIA SECURITY TIPSHEET

amazonstudios CONTENT SECURITY

Amazon Studios embraces social media and applies the same ethics, standards, and policies to the online world that employees are already expected to follow in the offline world. Given the broad reach and permanent nature of electronic communications, please follow this quick guide to help you participate in social media in a way that protects both you and Amazon.

Be smart when posting online. Approach online communications in the same way you approach physical communications – use sound judgment, common sense, and follow Amazon Studios Social Media Guidelines.

STOP, THINK, POST: BEWARE WHAT YOU SHARE!

SOCIAL MEDIA REQUIREMENTS FOR WORK

ACCOUNT MANAGEMENT

All business social media accounts must manage access permissions for all contributors. Ensure the proper set-up when managing social media accounts:

- Make login credentials unique to each individual who contribute to social media accounts.
- Enable two-factor authentication for all accounts where possible.
- Never share account profiles and credentials amongst contributors.
- Disable web browsers from storing and remembering passwords for social media sites.

ACCOUNT MANAGERS

Each production must designate an approver / administrator for each social media site. **Administrators/approvers must:**

- Track all accounts within a central Amazon Studios or production registry. The registry must NOT store any passwords.
- Initiate a quarterly review of approvers and users for each account.
- Review account access regularly to ensure that only approved individuals/devices are accessing the account.

PASSWORD REQUIREMENTS

Passwords must be configured to maintain high security on all social media accounts.

- Use unique passwords across all social media sites, so that the compromise of one account does not put another at risk.
- Use a full passphrase that contains at least 16 mixed characters.
- Switch out passwords regularly, at least every 3 months.

SOCIAL MEDIA RULES FOR PERSONAL USE

Never post the following to any personal (talent or crew) social media accounts (Facebook, Instagram, Twitter, LinkedIn, IMDB, YouTube, etc.) or to any online forum, blog post, or website:

- **SET PHOTOS** Photography is strictly prohibited on production sets.
- **PERSONAL PHOTOS** Never post pictures of talent, private events, project names, or references.
- **WORK INFORMATION** Details of contributions to a production or references to the production
- **FILMING LOCATIONS**
- **CONFIDENTIAL, NON-PUBLIC INFORMATION**
- **REFERENCES TO THE CAST OR CLIENTS**
- **SECURITY TITLES & CODE NAMES**
- Any pre-release content not yet available to the public
- Any other information or details that could compromise project confidentiality

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

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