

amazonstudios

CONTENT SECURITY

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 Policy (DP Note: link to URL, tbd)].

**BEWARE WHAT YOU SHARE!
WHEN IN DOUBT, DON'T POST!**

SOCIAL MEDIA USAGE 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



Talent photos, names, or references



Any references to the production



Filming locations



Confidential, non-public information



Any references to the cast or clients



Security titles / code names



Any pre-release content not yet available to the public



Any other pre-release content that could compromise project confidentiality

SOCIAL MEDIA USAGE FOR WORK

ACCOUNT MANAGEMENT

All business social media accounts must manage the access permissions and 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.



Account profiles and credentials should never be shared 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 quarterly to ensure that only approved individuals/devices are accessing the account.



PASSWORD REQUIREMENTS

If an individual who accesses an Amazon Studios social media account leaves the team or changes roles, then the registry must be updated accordingly, and a new password must be configured by his or her successor.



Passwords for each social media site must be different across accounts, so that the compromise of one account does not put another at risk.



Passwords contain a combination of upper / lower case, numeric, and special characters, (example of a strong passphrase Drink8GlassesofWater!).



The minimum password length must be 8 characters, and 16 character passphrases are highlight recommended!



Switch out passwords regularly, at least every 3 months.