Step 1

Secure Your Home Office

MINIMUM REQUIREMENTS

- Dedicate a workspace/office room specifically for production. Studio content should never leave the dedicated workspace.
- Position your monitors and any content away from the windows – if not possible, cover the windows while working.
- Limit access to your designated workspace, and supervise visitors (e.g. 3rd party personnel, cleaning service) at all times.
- Never use unencrypted thumb drives for data on the go. Storage devices must be encrypted and password protected. Content Security approves the usage of 256 AES drives with a pin code (e.g. Aegis Padlock).

RECOMMENDED SECURITY REQUIREMENTS

- Consider installing an alarm and security camera for entry/exit points.
- Consider installing a safe or lockbox (bolt or secure cable lock to something stationary if weighs less than 200lb) to store the encrypted drive when not-in-use

Reach out to content-security@amazon.com right away if any content loss or theft occurs.

amazonstudios CONTENT SECURITY

Step 2

Secure Your Device

Workstation Hardening Requirements

Set Auto Locks

Set your device to automatically lockout after 10 minutes of inactivity.

Encrypt

Secure your device by applying encryption. FileVault for Mac or Bitlocker for Windows

Protect Against Viruses

Subscribe to Antivirus software such as Sophos or TrendMicro, and scan your device regularly.

Limit Vulnerabilities

Disable Applications that are not in use.

Enable Firewalls

Turn on your local firewalls for both Mac and PC devices

Protect External Storage

Block USB mass storage connection points via a EndPoint Protector solution.

amazonstudios CONTENT SECURITY

Step 3

Secure Network Connections

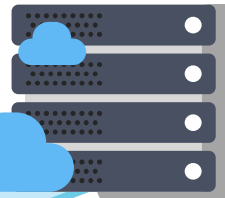
For: Marketing, Clearance

Production/High Security Network

Access Control

- Dedicated production VPN user group - these users cannot VPN to company/corp network that has internet access
- Storage access also restricted
- Enable firewall geo-restriction services if available

Internet Connection



VPN into the Network

- 2FA
- Disable Split tunneling
- AES 256 encryption

Log on with

Your Hardened Workstation

Step 3

Secure 3rd Party Connections

For: VFX, Editing

Production/High Security Network

Log on with
Your Hardened Workstation

Approved Solutions
- Teradici
- Sohonet Clearview
- Evercast
- Bebop Technology

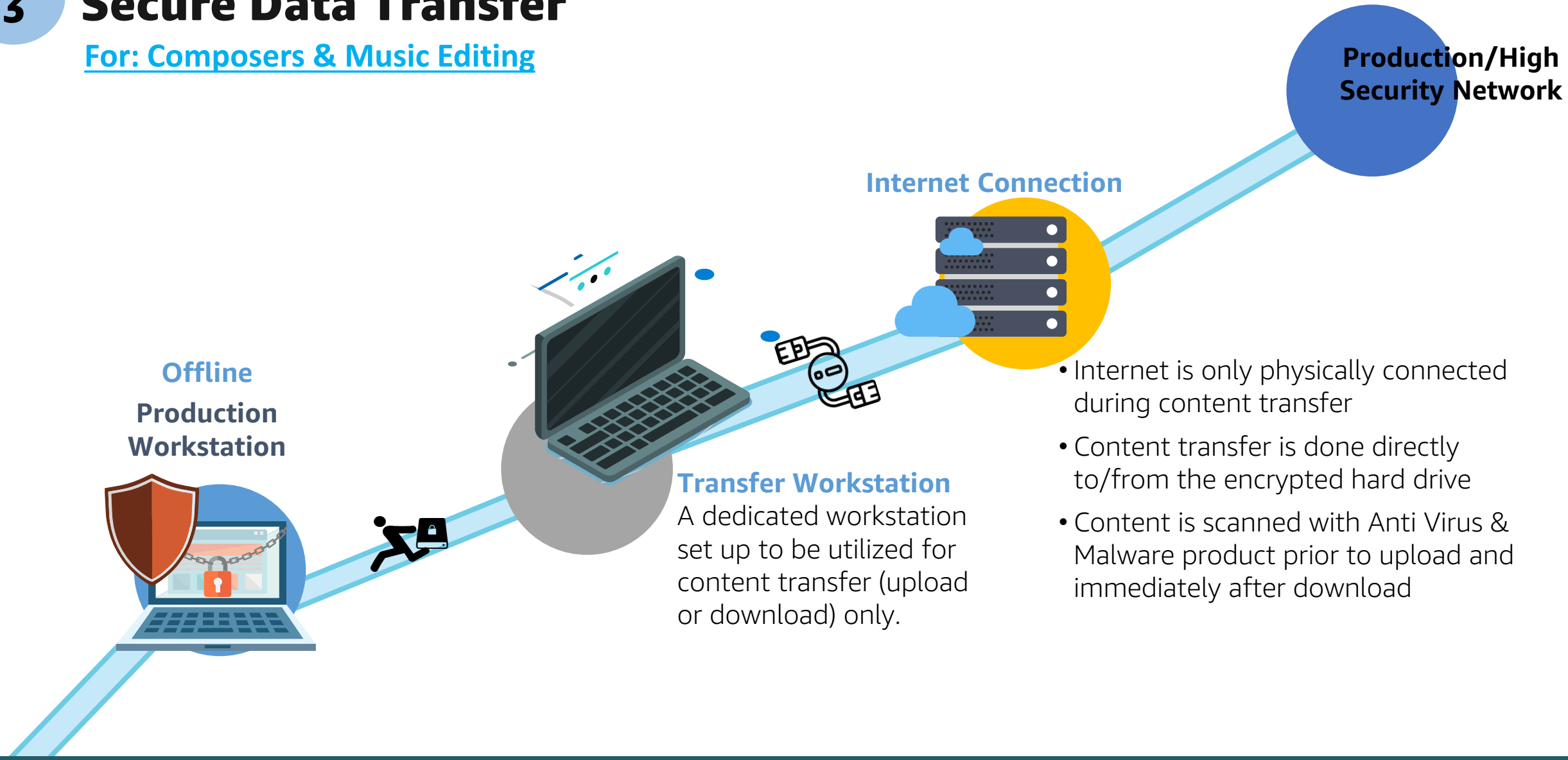
Access Control
- 2FA
- Disable Split tunneling
- AES 256 encryption

Note: Please reach out to Amazon Content Security if you do not see a solution that you would like to leverage

Step 3

Secure Data Transfer

For: Composers & Music Editing



Approved Cloud Solutions for Amazon Originals

Preferred Solutions for:

- Sharing Within the Production
- Sharing Between Production/Amazon/Vendors
- Storage

Approved Solution

I need to share/send/store the following:

Approved Solutions	Admin & Prod Docs	Art	BTS & Prod Videos	Comms & Logistics	Cont. Photos	Creative Docs	Franchise Photos	Prod Photos	Scripts	Sound	VFX	Watermarking Capability
Box	Storage	Sharing + Storage	Approved		Approved	Sharing + Storage	Approved	Sharing		Approved	Approved	Settings controlled by User
Box Capture					Approved		Approved	Approved				Settings controlled by User
Chime	Approved			Approved								No watermarking capability, manual watermark required
Email				Approved								No Assets should be sent or stored in Email
Global Edit						Sharing + Storage						Settings controlled by User
Originals Access		Sharing Between	Sharing + Sharing Between			Sharing Between	Sharing Between	Sharing Between		Sharing + Sharing Between	Sharing + Sharing Between	Automatic
Quantum Storage or PixIt		Approved	Storage			Approved		Storage		Storage	Sharing + Storage	No watermarking capability, manual watermark required
S3											Storage	No watermarking capability, manual watermark required
Scenechronize	Sharing + Storage			Approved					Sharing + Storage + Sharing Between		Storage	Automatic
SyncOnSet					Storage							Automatic