EXHIBIT

CONTENT PROTECTION REQUIREMENTS

1. Service Provider shall not, nor shall it permit or authorize its employees, contractors or other personnel ("Service Provider Personnel") to, copy, transfer, publish, relinquish possession of, reveal, exploit, or allow third-party access to, any scripts, images, storyboards, style guides, marketing and promotional content, film, video and/or digital elements containing any content from or related to theatrical motion pictures, television shows, animation, video games and other works created, owned and/or controlled by WarnerMedia ("**WM**") or any of its affiliates, ("**WM Content**") regardless of the form in which such WM Content exists, except as strictly necessary to perform services under this Agreement. Service Provider shall remain responsible for such WM Content from the time Service Provider obtains possession of WM Content until it is returned to WM's possession, delivered to another location designated by WM in writing, or destroyed pursuant to WM's specific written instructions.

2. Service Provider shall establish and employ such physical, electronic and organizational security procedures and policies that are compliant with Motion Picture Association content security best practices (https://www.motionpictures.org/what-we-do/safeguarding-creativity/additional-resources/) ("**MPA Best Practices"**), as are applicable to Service Provider's facility(ies). Service Provider shall also complete (1) the appropriate WM Content Security Questionnaire ("Questionnaire") and (2) if required by WM, the Trusted Partner Network (https://www.ttpn.org/) assessment and (3) obtain approval of Service Provider's content security procedures and policies from WarnerMedia Content Security (contentsecurity@warnermedia.com) all prior to the execution to this Agreement. Service Provider shall immediately notify WM of any changes to its physical, electronic or organizational security procedures and policies if such changes would result in Service Provider being out of compliance with the MPA Best Practices and/or would be inconsistent with any information provided in the Questionnaire.

3. Service Provider shall not remove or modify any burn-in warnings or watermarks included on physical or digital assets containing or embodying WM Content.

4. Service Provider shall advise in writing all Service Provider Personnel of Service Provider's content security procedures and policies and that criminal and/or civil liability may potentially arise by reason of the piracy, theft, unauthorized copying, recording, distribution or other unauthorized use of WM Content. Service Provider shall keep a written record of all Service Provider Personnel who have access to WM Content and shall provide such information to WM on request. Service Provider shall conduct background checks on Vendor Personnel to the extent permitted by law prior to such Service Provider Personnel being given access to WM Content and/or Service Provider systems which would allow access to WM Content. Service Provider will take all reasonable steps to minimize the risk of Vendor Personnel creating a security-related risk to WM Content. In all cases, Service Provider shall be responsible for verifying (a) the identity of all Service Provider Personnel, and (b) the information provided by Service Provider Personnel in any application to be engaged by Service Provider, including without limitation their employment history. Service Provider shall not allow anyone to work on, or have access to, WM Content, in the event that any verification, background check or other information known to Service Provider indicates at any time that any such individual (i) has engaged in any misconduct or offense involving dishonesty, (ii) any repeat or regular pattern of misconduct, or (iii) may otherwise pose a security-related risk to WM or WM Content.

5. Service Provider shall assign one individual within its facility who shall be principally responsible for the security of WM Content and shall provide WM with the name and contact information for that individual. The responsible individual shall be familiar with these Requirements and shall maintain a log of assets disseminated within Service Provider 's facility including identification of individuals receiving such assets. Service Provider shall also identify and provide to WM the name and contact information for Vendor's executive responsible for all security measures.

6. WM and/or its representative shall have the right, during business hours and on reasonable notice, to conduct a security site survey or otherwise inspect Service Provider 's facilities to confirm Service Provider's compliance with this Exhibit. WM and/or its representative shall comply with the security requirements of Service Provider; provided, however, that such security requirements do not interfere with WM's right to inspect hereunder. Service Provider shall at no cost to WM, within thirty (30) days from written notice from WM, comply with any request that Service Provider remediate any non-compliance (such non-compliance to be in the sole opinion of WM) with the MPA Best Practices identified as a result of the security survey, provided, however, that such remediation shall not be deemed a right of cure and nothing herein shall derogate from WM from taking any other action to which it is entitled in the event of non-compliance. Service Provider agrees, in consultation with WM, to implement such additional security measures as WM may require to protect WM Content from time to time.

7. Service Provider shall immediately (*i.e.*, in no less than 24 hours) notify WM by phone and e-mail (including to protect@warnerbros.com) regarding any loss, theft, injury, unauthorized access, copying, recording, distribution or other unauthorized use of WM Content or of any other breach of security at Service Provider's facilities whether or not such breach involves WM Content ("Incident"). Notwithstanding any other provisions of this Agreement, if the Incident occurred in whole or in part due to Service Provider 's lack of establishment and/or execution of security procedures required by this Agreement, Service Provider shall be liable for any and all damages arising from the Incident, including attorney's fees that may be incurred by WM to investigate the Incident or otherwise enforce the obligations hereunder. Service Provider shall use best efforts, at Service Provider r's own cost and expense, to recover all lost or stolen materials. Service Provider shall conduct a prompt investigation concerning the occurrence and cause of the Incident and the steps required to remediate the Incident and fully report the result of such investigation to WM.

8. Service Provider 's use of electronic file delivery or other access methods to transfer WM Content between facilities or to/from WM shall be subject to WM's prior written approval. If electronic file transfer is approved by WM, Service Provider shall employ (i) no less than 256-bit encryption, or the maximum allowed by local law in the territory, (ii) password access to secure sites, (iii) maintenance of a user database in compliance with all applicable laws and regulations, and (iv) system administration of the service/system utilized to post and pull-down files. Service Provider shall confirm deletion of any WM Content located on servers upon completion of the subject project.