Compliance and Robustness Rules
For Media Streaming Content Protection

These Compliance and Robustness Rules shall apply as specified below to use of Licensed Software and Keys provided under license from Adobe to provide server-based software for the protection of streamed audiovisual content and the distribution of Content Licenses to allow access to and consumption of such protected content streams. These Compliance and Robustness Rules are not applicable to the use of Adobe licensed software in client devices that allow for decryption and consumption of such content.

All capitalized terms not defined in Section 1 shall have the meaning defined in the relevant Adobe license agreement under which you are using the Licensed Software and Key for the foregoing purposes and required to comply with these Compliance and Robustness Rules.

1. Definitions.

1.1. "Media Streaming Content Protection" means the RTMPe and SWF Verification libraries in obfuscated source or object code form, and any related code and Documentation licensed by Adobe.

1.2. " Key" means a cryptographic value embedded in the Licensed Software by Adobe that is used to establish trust between server and client.

2. Compliance Rules.

2.1. **Permitted Use**. The Licensed Software shall be used solely for the purpose of protecting audiovisual content for consumption by authorized Adobe Runtimes.

2.2. **No Modification of APIs.** The Licensed Software shall not be modified or to make the functionality of the Licensed Software available to other software applications not licensed by Adobe.

2.3. **No Modification or Replacement of Key**. The Key embedded in the Licensed Software by Adobe shall not be modified or replaced.

2.4. **No Key Extraction.** Licensee shall not extract a Key from the Licensed Software, regardless of whether provided by Adobe in binary, object, or source code form, and separately record, transcribe, reproduce or disseminate such Key in any form, either internally or externally

2.5. **Secure Handling of Highly Confidential Information.** Licensee shall comply with the following requirements concerning access to and handling of Highly Confidential Information:

(i) Highly Confidential Information shall be stored and used only at Authorized Sites. The rooms within the Authorized Sites in which Highly Confidential Information is stored or used must at all times be secured by lock and key, electronic card access or similar measures, and access-controlled, such that a verifiable log of all those having access to, and the times of entering and leaving such rooms is created and preserved for a minimum of one year.

(ii) Only Authorized Employees shall have access to copies of Highly Confidential Information in permanent or temporary storage of any kind. The use of the Highly Confidential Information by the Authorized Employees shall be strictly limited to

the purpose of the Agreement under which Licensee received the Licensed Software.

(iii) When not in use, Authorized Employees shall permanently store the Highly Confidential Information only in a safe or password protected computer accessible only to Authorized Employees. Authorized Employees may remove or copy Highly Confidential Information from such permanent storage and make temporary copies onto computers or devices located within the Authorized Facilities as needed for the purposes contemplated by the Agreement under which Licensee received the Licensed Software provided that when the Highly Confidential Information is stored on such a computer or device, such computer or device shall be secure and password-protected. Authorized Employees must have a separate unique, non-trivial, non-obvious password for each permanent or temporary storage location that is changed with reasonable frequency in accordance with industry best practices. Licensee shall maintain and take reasonable security measures to preserve the integrity of log records recording the date and time at which keys are copied to or deleted from each temporary computer or device and permanent storage site, and the identify of the Authorized Employee performing such deletion or copying, such that an auditor examining such records can determine the number and location of all copies of keys at any point in time over the previous two years.

(iv) Authorized Employees must adhere to a "clean desk" policy at their facilities at an Authorized Site. "Clean desk" policy means the Highly Confidential Information must be completely and permanently deleted from any computer or device and stored consistent with 2.5(iii) when not in use.

(v) Licensee shall not let the Highly Confidential Information be viewed, used, copied, disseminated, or in any way circulated to any individual other than to Authorized Employees.

(vi) Adobe may inspect the Authorized Sites, including the computing systems and Licensee's Authorized Sites to verify compliance with the provisions of this Section 2.5 upon reasonable notice to Licensee, as applicable, and in compliance with the reasonable policies of such Licensee relating to access.

3. Robustness Rules.

3.1. **Protection of HCI.** Licensee facilities shall be designed and operated in a manner that is clearly designed to effectively frustrate attempts by unauthorized parties to obtain and use HCI in an unauthorized manner or to modify or replace Keys contrary to Section 2.3.