Compliance and Robustness Rules

For Adobe Flash Access 2.0, 3.0 and Adobe Access 4.0 or later versions

These Compliance and Robustness Rules shall apply as specified below to use of Flash Access Licensed Software and Certificates provided under license from Adobe to provide server-based services for the protection of Content and the distribution of Content Licenses to allow access to and consumption of such protected content. 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 Certificates (the "License Agreement") for the foregoing purposes and required to comply with these Compliance and Robustness Rules.

All references to "Content Distributor or Hardware Customer, if applicable" may be disregarded if Licensee is not providing a hosted Service or Hardware Product to third parties for the protection of Content and the distribution of Content Licenses. If Licensee is providing a hosted Service, then all such references state obligations that must be met by each Content Distributor, i.e., all such requirements are applicable to each Content Distributor. If Licensee is distributing Hardware Product, then all such references state obligations that must be met by each Hardware Customer, i.e., all such requirements are applicable to each Hardware Customer for each unit of the Hardware Product.

1. **Definitions.**

   1.1. "Adobe Access" means Adobe Flash Access or Adobe Access branded software licensed by Adobe.

   1.2. "Sensitive Keys" means Root Public Keys and Private Keys.

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

   1.4. "Sensitive Data" means server configuration files, Sensitive Keys and Content Encryption Keys.

   1.5. "Hardware Customer" for the purposes of these Compliance and Robustness Rules, shall mean the end user of a hardware device with a fully integrated version of the Adobe Access software.

2. **Compliance Rules.** These Compliance Rules set forth mandatory conduct requirements for Licensee (and Content Distributors or Hardware Customer, if applicable).

   2.1. **Permitted Use**. The Licensed Software and Certificates shall be used solely for the purpose of creating and distributing Protected Content intended for decryption and rendering on client devices using an Adobe Runtime.

   2.2. **Trusted Packagers**. Licensee shall not issue a Content License for a specific instance of Protected Content unless the Licensed Server issuing such Content License has verified the Certificate of the Packager that encrypted such Protected Content.

   2.3. **Certificates and Certificate Revocation Lists**. Licensee (and Content Distributor or Hardware Customer, if applicable) shall not use certificates issued by parties other than Adobe to substitute for Certificates when using the functionality of the Licensed Software. Licensee (and Content Distributor, if applicable) shall not modify or otherwise interfere with the automated mechanism by which the Licensed Software periodically obtains from Adobe and uses the most up to date CRL, or take any action to use a CRL with the Licensed Software that is not the most current available from Adobe.

2.4. **Distribution of Certificates**. Certificates shall not be distributed to any entity other than the entity for which Adobe issued them, except insofar as the Licensed Software in normal operation incorporates a Certificate in files sent to an authorized Consumer of Protected Content.

2.5. **No Modification of APIs**. The Licensed Software shall not be modified so as to alter the behavior of any API or to make the functionality of the Licensed Software available to software applications other than licensee's Licensed Product.

2.6. **Distribution of Compliance and Robustness Rules**. Licensee (and Content Distributor or Hardware Customer, if applicable) shall provide a copy of these Compliance and Robustness Rules to each person involved in or responsible for the operation of any server containing any portion of the Licensed Software, Certificates, or Private Keys.

2.7. **No Extraction of Content Encryption Keys**. A Licensee shall not extract a Content Encryption Key from Protected Content packaged by another Licensee or a Content Distributor and separately record, transcribe, reproduce or disseminate such Content Encryption Key in any form.

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

2.9. **No Private Key Distribution**. Licensee, Content Distributors and Hardware Customers shall not distribute a Private Key to another entity in any form.

2.10. **Secure Handling of Highly Confidential Information**. Licensee (and Content Distributor or Hardware Customer if applicable) shall comply with the following requirements concerning access to and handling of Highly Confidential Information (Private Keys):

(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 License Agreement.

(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 License Agreement, 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 (and Content Distributor or Hardware Customer, if applicable) 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 Section 2.10 (iii) when not in use.

(v) Licensee (and Content Distributor or Hardware Customer if applicable) 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) Upon expiration of a Certificate, Licensee (or Content Distributor or Hardware Customer, if applicable) shall securely delete and destroy all copies of the Private Key relating to such Certificate in its possession, except and only to the extent that such Private Key remains necessary to issue authorized new Content Licenses for previously distributed Protected Content. Upon expiration or termination of the License Agreement, Licensee (and Content Distributor or Hardware Customer, if applicable) shall securely delete and destroy all copies of Highly Confidential Information in its possession.

(vii) Adobe may inspect the Authorized Sites, including the computing systems and Licensee's (or Content Distributor's or Hardware Customer, if applicable) Authorized Sites to verify compliance with the provisions of this Section 2.10 upon reasonable notice to Licensee (or Content Distributor or Hardware Customer, if applicable) and in compliance with the reasonable policies of such Licensee (or Content Distributor or Hardware Customer, if applicable) relating to access.

3. **Robustness Rules.** These Robustness Rules set forth mandatory processes and standards of protection for Licensee (and Content Distributors or Hardware Customer, if applicable) to maintain the integrity and security of Sensitive Data.

3.1. **Level of Protection for Sensitive Data**. Licensee's Licensed Product and facilities (and Content Distributor's or Hardware Customer's facilities, if applicable) shall be designed and operated in a manner that is clearly designed to effectively frustrate attempts by unauthorized parties to obtain and use Sensitive Data in an unauthorized manner or to modify Root Public Keys contrary to Section 2.7. Such Licensed Products and facilities shall be designed and operated such that anyone gaining unauthorized access thereto:

3.1.1. Cannot compromise the confidentiality or integrity of Sensitive Data merely by obtaining unauthorized access (either physical or logical) to the facilities or merely by using generalpurpose tools or equipment that are widely available (including being available on the Internet) at a reasonable price such as screwdrivers, jumpers, clips, soldering irons, packet sniffers, port scanners, vulnerability scanners, exploit scripts, software capable exploiting replay attacks, dictionary attacks and information gathered using search engines ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers ("Specialized Tools"), other than devices or technologies that are designed or made available for the specific purpose of bypassing or circumventing the Content Protection Functions ("Circumvention Devices").

3.1.2. Can only with difficulty compromise the confidentiality or integrity of Sensitive Data using professional tools or equipment, such as logic analyzers, chip disassembly systems, or incircuit emulators or any other tools, equipment, methods, or techniques not described in Section 3.1.1, such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

3.2. **Methods of Protection**. Licensee (and Content Distributor or Hardware Customer, if applicable) shall comply with at least each of the following specific provisions in order to secure the levels of protection set forth in 3.1:

3.2.1. **Secure Deployment Guidelines**. Licensee (and Content Distributor or Hardware Customer, if applicable) shall review the recommendations of Adobe's Secure Deployment Guidelines for Adobe Flash Access 2.0 and employ methods of protection against unauthorized access to and use of Sensitive Data that are described therein or alternative methods that are at least as effective. If such unauthorized access and use occurs under circumstances in which following Adobe's recommendations would have prevented such unauthorized access and use, the alternative means of protection employed are not in compliance with this Section 3.2.1

3.2.2. **Software and Hardware Methods**. Licensed Products shall be designed and operated using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to compromise the confidentiality or integrity of Sensitive Data, as set forth below in Sections 3.2.2.1, 3.2.2.2 and 3.2.2.3:

3.2.2.1. **Software**. For the purposes of these Compliance and Robustness Rules, "Software" shall mean any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Any portion of the Licensed Product consisting of Software that is capable of accessing the Sensitive Data in usable form shall:

3.2.2.1.1. Comply with Section 3.1 by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in privileged or supervisor mode, execution on a hardened operation system, and/or embodiment in a secure physical implementation.

3.2.2.1.2. Be designed so that checking of the integrity of the component parts occurs such that modifications must be identified and processes will promptly assess whether these modifications were authorized or unauthorized. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Section 3.1. The Licensee shall describe in the security policy, standards and procedures (as described in section 3.3) how this provision is satisfied.

3.2.2.2. **Hardware**. "Hardware" shall mean a physical device, including a component, that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such physical device or component where such instructions or data have been customized for such Licensee and/or can only be accessed under the control of the Licensee by authorized parties. Any portion of the Licensed Product consisting of Hardware that is capable of accessing the Sensitive Data shall:

3.2.2.2.1. Comply with Section 3.1 by any reasonable method including but not limited to embedding Sensitive Data in a Hardware Security Module (HSM) that provides the level of protection described in section 3.1 Licensees that wish to employ an HSM should use an HSM that meets FIPS 140-2 Level 3 or higher, or an equivalent level of protection as defined in an alternative internationally accepted standard.

3.2.2.2.2. Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would permit unauthorized access to or use of Sensitive Data would pose a serious risk of rendering the Licensed Product unable to create Protected Content or issue Content Licenses and would be promptly detected as described in section 3.2.2.1.2.

3.2.2.3. **Hybrid**. The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection, which would be provided by a pure Software implementation.

Construction—Defeating Functions. Licensed Products shall not include: (a) switches, buttons, jumpers or software equivalents thereof, (b) specific traces (electrical connections) that can be cut, or (c) functions (including service menus and remote-control functions), in each case by which the Sensitive Data in such Licensed Products can be accessed in usable form.

3.3. **Risk Prevention Policy**. Licensee (and Content Distributor or Hardware Customer, if applicable) shall create, maintain and implement a written policy, including periodic self-audits, consistent with or intended to accomplish that same purpose as the guidelines in ISO/IEC 27001:2005 and 27002:2005, detailing the security objectives and methods that are implemented in order for

its Licensed Products and facilities to comply with these Compliance and Robustness Rules. Licensee (and Content Distributor or Hardware Customer, if applicable) shall perform a formal assessment including, but not limited to, the threats listed in section 3.3.2 ("Threat Assessment"). The Threat Assessment must be reviewed by a qualified third party and documented with an attestation statement, unless waived in writing by Adobe. The threat assessment should anticipate and protect against unauthorized access to, modification or use of the Sensitive Data via the specific threats listed below, provided that this is not an exhaustive list and Licensee (and Content Distributor or Hardware Customer, if applicable) should consider and include in their policy additional threats that might apply to their specific Licensed Products and facilities:

3.3.1 ISO 27001:2005 and 27002:2005

- Unauthorized physical access to any Licensed Product and facility components
- Destruction of any or all such component(s) by accident or design
- Availability compromised by physical disconnection or other physical intervention
- Modification or interruption of power supplies and network connections
- Faults in vendor's software operating systems or applications
- Mis-configuration of vendor's software
- Unauthorized modification of operational log files
- Eavesdropping on local networks, for example using a protocol analyzer (hybrid threat)

3.3.2 Threat Assessment:

- Unauthorized access to Licensed Products via a console or a network terminal.
- Man in the middle attacks.
- Destruction of key material.
- Installation of eavesdropping facilities on system components.
- Improper or unauthorized creation, modification or deletion of user accounts.
- Improper or unauthorized creation, modification or deletion of database contents.
- Improper or unauthorized creation, modification or deletion of database access controls.
- Exploitation of input control (buffer overflows) to undermine availability and escalate privilege.
- Unauthorized acquisition of cipher and/or plaintext
- Obtaining unauthorized access by misrepresentation ("social engineering")

3.4. **Advance of Technology**. Although a Licensed Product when designed and first shipped or facilities when first designed and used may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design, would have caused such Licensed Products or facilities to fail to comply with this Section 3 ("New Circumstances"). If a Licensee (or Content Distributor or Hardware Customer, if applicable) has actual notice or actual knowledge of New Circumstances, then as soon as commercially reasonably possible, and in any event no later than eighteen (18) months after such actual notice or knowledge, such Licensee or Content Producer shall cease use and distribution of the Licensed Product or use of the facilities that are not compliant with Section 3 in view of the then-current circumstances, and shall only use and distribute Licensed Products or use facilities that are compliant with Section 3 in view of the then-current circumstances.