Shared Web Data Security & Service Level Agreement

The manner by which Ansys provides access to Shared Web Licensing shall be at Ansys' discretion, may change over time and, in any case, shall require Customer to be connected to the internet. Subject to the exceptions listed below, Ansys will use commercially reasonable efforts to make Shared Web Licensing available 99.9% of the time during each calendar month during the License Term (referred to herein as the "Availability Commitment"). The availability of Shared Web Licensing for a given month will be calculated according to the following formula (referred to herein as the "Availability"):

Where Total minutes in the month = TMM

Total minutes in the month the services are unavailable = TMU

Availability = ((TMM-TMU) X 100)/TMM

And total days in the month the services are unavailable = TDU = (TMU / 1440).

For purposes of this calculation, Shared Web Licensing will be deemed to be unavailable (referred to herein as "Unavailable") only if Shared Web Licensing does not respond to HTTP requests issued by Ansys' monitoring software. Further, Shared Web Licensing will not be deemed Unavailable for any downtime or outages that result from the following exceptions:

Shared Web Licensing will not be considered as Unavailable (and minutes will not accrue as TMU) for any downtime or outages that result from any maintenance performed by Licensor or Licensor's cloud hosting providers, which shall be communicated to Licensee from time to time (collectively referred to herein as "Scheduled Maintenance"). In the event during the License Term that Ansys does not meet the Availability Commitment, as Licensee's sole and exclusive remedy for such failure, Licensee may be entitled to be compensated with a pro-rated credit equal to one (1) day for each day that the Cloud License Service is Unavailable beyond the Availability Commitment (TDU), including any fractional amounts (the "Licensee Credit"). For example, if the Cloud License Service is Unavailable for 30 minutes beyond the 99.9% Availability Commitment, then Licensee may be entitled to a pro-rated credit of 1 day. To be eligible for a Licensee Credit, Licensee must request a Licensee Credit from Ansys: i) within thirty (30) days from the date that Ansys failed to meet the Availability Commitment as set forth herein; and ii) during the License Term. Licensor shall make the Availability status of the Cloud License Service available to Licensee.

1. Licensor, upon reasonable notice to Licensee, at Licensor's own cost and no more than one (1) time per year, may have a third party independent auditing firm review and examine license usage under this Agreement and for that purpose such third party firm shall be entitled to have access to Licensee's premises at a mutually agreeable time and have access to all relevant data, files and information. Such third party firm shall not have physical access to Licensee's computing devices in connection with any such audit, without Licensee's prior consent, which shall not be unreasonably withheld. Licensee will reasonably cooperate with such third-party auditor's activities under this Agreement.

2. As part of the web licensing services Ansys will process limited personal data as further outlined in the applicable Ansys Data Processing Addendum and information relating to Ansys software that has been accessed through the web licensing service. Ansys will use such information to (i) provide the service, (ii) improve product performance, resource allocation, and support, and (iii) analyze, support, and/or optimize your or your employing entity's use of Ansys product and services.

ANSYS SHARED WEB LICENSING SECURITY ADDENDUM

This Ansys Shared Web Licensing Security Addendum (the "Shared Web Security Addendum") is incorporated into and made a part of the Shared Web Licensing Terms (the "Terms"). Capitalized terms used but not defined herein shall have the meaning set forth in the Terms. In the event of any conflict between the Terms and this Shared Web Security Addendum, this Shared Web Security Addendum shall govern.

1. Definitions

a. "**Security Incident**" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Cloud License Service.
b. "**Security Industry Standards**" means, the International Organization for Standardization ("**ISO/IEC**") 27001, ISO/IEC 27002:2013, and the US National Institute of Standards and Technology ("**NIST**") Cyber Security Framework (and any supporting NIST standards such as 800-44).

2. Governance

a. Policies and Standards- Ansys shall maintain a risk-based security program based on the Security Industry Standards to systematically manage and protect the Cloud License Service (the "**Ansys Security Program**").
b. Ansys Security Program- The Ansys Security Program is aligned to the Security Industry Standards and is implemented on an organization-wise basis. As part of the Ansys Security Program, Ansys shall:
    i. Maintain a security committee comprised of leaders across business units that oversee the Ansys Security Program;
    ii. Assign appropriate roles for developing and managing the Ansys Security Program and furthering the security, confidentiality, and integrity of the Cloud License Service;
    iii. Ensure that personnel supporting the Cloud License Service are sufficiently trained, qualified, and experienced to fulfill their roles and functions; and
    iv. Train such employees upon hire and periodically thereafter.

3. Purpose and Scope

a. Purpose- Ansys is committed to maintaining a comprehensive security and data protection program to secure and maintain the Cloud License Service. This Shared Web Security Addendum outlines the technical and organization safeguards that ensure the security and integrity of the Cloud License Service. Notwithstanding anything in the Terms or this Shared Web Security Addendum to the contrary:
    i. The terms outlined in this Shared Web Security Addendum shall apply only to the Cloud License Service and shall not apply to any other product or service offered by Ansys; and
    ii. Ansys has no obligation to review or assess the Licensee information to identify information subject to any specific legal, regulatory, or other requirements.
b. Licensee Responsibilities- Licensee acknowledges and agrees that Licensee shall be responsible for:
    i. Determining whether the Cloud License Service are suitable for Licensee's use;
    ii. Implementing and managing security measures to secure Licensee's access and use of the Cloud License Service; and
    iii. Managing and protecting its access to the Cloud License Service.

4. Data Retention

a. Data Retention- During the License Term, Licensee is solely responsible for managing the deletion of its Named Users' accounts and access to Cloud License Service. Notwithstanding the foregoing, after a period of thirty (30) days from the termination or expiration of the Terms, Ansys may remove all user information from the Cloud License Service.

5. System Security

a. Cloud License Service Encryption- The Cloud License Service leverages industry-standard encryption methods to protect data within the Cloud License Service in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss.
b. Network Security- Ansys shall maintain commercially reasonable controls, policies, and technologies to protect the Ansys network including firewalls, VPN, and intrusion protection and monitoring systems.

6. Operational Security

a. Business Continuity and Disaster Recovery- Ansys shall maintain processes and procedures designed to ensure the Cloud License Service remain resilient in the event of a failure. Such plans shall be periodically reviewed and updated as part of the Ansys Security Program.
b. Development- Ansys shall (i) make commercially reasonable efforts to prevent, at the time of delivery, the introduction of any viruses, time bomb, trojan horse, or other intentionally destructive or disabling devices into the Cloud License Service, and (ii) conduct virus scanning and penetration testing on the Cloud License Service prior to its release.
c. Third Party Security- Ansys shall (i) conduct commercially reasonable due diligence on its third-party service providers to confirm their ability to meet applicable security requirements and compliance with applicable laws and regulations, and (ii) ensure that all third-party service providers are under contractual agreements containing terms and conditions similar to this Shared Web Security Addendum.

7. Administrative Controls

a. Access Controls- To ensure that access to the Cloud License Service is limited, Ansys will:
    i. Maintain technical and organizational controls to limit access to Cloud License Service;
    ii. Implement controls to authenticate Named Users; and
    iii. Maintain multi-factor authentication for Ansys employees.
b. Information Security Policies- As part of the Ansys Security Program, Ansys shall:
    i. Maintain information security policies that govern the Ansys Security Program and the obligations and responsibilities of Ansys employees; and
    ii. Review and update its information security policies at regular intervals to ensure their continuing suitability, adequacy, and effectiveness.

8. Physical and Environmental Controls

a. Physical Security- Licensee acknowledges and agrees that Ansys does not maintain physical data centers to support the Cloud License Service. Ansys conducts regular due diligence on its cloud service providers (which includes reviewing applicable industry standard reports and verifications of such providers) to assess whether the providers have appropriate security controls addressing the security, integrity, and availability of the Cloud License Service. Such controls shall include, but are not limited to:
    i. Physical access to the facilities is controlled at building ingress points;
    ii. Physical access to servers is managed by access control devices;
    iii. Physical access privileges are reviewed regularly;
    iv. Facilities utilize monitor and alarm response procedures;
    v. Facilities utilize fire detection and protection systems;
    vi. Facilities utilize power back-up and redundancy systems; and
    vii. Facilities utilize climate control systems.

9. Incident Response

a. Security Incident Response Policy- Ansys shall maintain documented policies and procedures that govern the investigation and response to Security Incidents and required remediation and/or mitigation actions.
b. Notice- In the event of a Security Incident, Ansys shall notify Licensee without undue delay. A notification

required under this Section 9 will include, to the extent available:

i. A description of the nature of the Security Incident, and
ii. A description of the measures taken (or proposed to be taken) to address the Security Incident.

10. Assessments

a. Service Assessments- With respect to the Cloud License Service, Ansys shall:
   i. Periodically assess the Cloud License Service to analyze existing security risks, identify new risks, and evaluate the effectiveness of existing security controls;
   ii. Ensure that penetration and vulnerability tests are periodically performed on the Cloud License Service; and
   iii. Implement procedures to document and address vulnerability discovered during the testing outlined in 10(a)(i) and (ii).

11. Miscellaneous

a. Updates- Ansys may update, without notice, the Ansys Security Program, this Ansys Shared Web Security Addendum, and the technical and organizational safeguards designed to secure the Cloud License Service, provided that such updates shall not result in a material degradation of the security of the Cloud License Service.