Ansys Cloud Platform Security Addendum

(v5.17.24)

This Ansys Cloud Security Addendum (the "**Cloud Security Addendum**") outlines the technical and organizational security measures for the Ansys Cloud Platform. Capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Cloud Security Addendum, this Cloud Security Addendum shall govern.

1. Definitions

a. "**Customer Data**" means geometries, simulation, and simulation results data submitted or accessed by the Customer while using the Ansys Cloud Platform.
b. "**Security Incident**" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.
c. "**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. Purpose and Scope

a. Purpose- Ansys is committed to maintaining a comprehensive security and data protection program to secure and maintain the Ansys Cloud Platform and the Customer Data. This Cloud Security Addendum outlines the technical and organization safeguards that ensure the security and integrity of the Ansys Cloud Platform and the Customer Data. Notwithstanding anything in the Agreement or this Cloud Security Addendum to the contrary:
    i. The terms outlined in this Cloud Security Addendum shall apply only to the Ansys Cloud and shall not apply to any other product or service offered by Ansys; and
    ii. Ansys has no obligation to review or assess the Customer Data to identify information subject to any specific legal, regulatory, or other requirements.
b. Customer Responsibilities- Customer acknowledges and agrees that Customer shall be responsible for:
    i. Determining whether the Ansys Cloud Platform is suitable for Customer's use;
    ii. Implementing and managing security measures to secure Customer's access and use of the Ansys Cloud Platform;
    iii. Managing and protecting its User roles and credentials including: (1) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (2) reporting to Ansys if a User's credentials have been compromised, (3) appropriately configuring User and role-based controls, and (4) maintaining appropriate password uniqueness, length, complexity, and expiration; and

    iv. Requesting Customer Data from the Ansys Cloud Platform after termination of the Agreement.

3. 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 Ansys Cloud Platform and Customer Data (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 Customer Data;
    iii. Ensure that personnel supporting the Ansys Cloud Platform are sufficiently trained, qualified, and experienced to fulfill their roles and functions; and
    iv. Train such employees upon hire and periodically thereafter.

4. Data Retention

a. Data Retention- Unless required by law, Ansys will not delete or export any Customer Data from the Ansys Cloud Platform, and it is Customer's responsibility to ensure that the Customer Data is removed prior to the termination of the Agreement. Notwithstanding the foregoing, after a period of thirty (30) days from the termination or expiration of the Agreement, Ansys may delete the Customer Data from the Ansys Cloud Platform.

5. System Security

a. Encryption of Customer Data- All Customer Data is encrypted both in transit and at rest using a symmetric key pair (AES 256 based), which is downloaded via an authenticated REST API call over HTTPS/TLS. The Customer Data is then encrypted via asymmetric key.
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.
c. Data Segregation- Ansys shall maintain logical, operational, and technical controls to ensure the separation of Customer Data from Ansys data and the data of other Ansys customers.

6. Operational Security

a. Business Continuity and Disaster Recovery- Ansys shall maintain processes and procedures designed to ensure the Ansys Cloud Platform 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 into any Program(s) of any viruses, time bomb, trojan horse, or other intentionally destructive or disabling devices, and (ii) conduct virus scanning of all Program(s) prior to the release of such Program(s).

c. Third Party Security- Ansys shall conduct commercially reasonable due diligence on its third-party service providers to confirm their ability to meet applicable security requirements and compliance applicable laws.

7. Administrative Controls

a. Access Controls- To ensure that access to Customer Data is limited, Ansys will:
   i. Maintain technical and organizational controls to limit access to Customer Data;
   ii. Implement controls to authenticate Ansys employees and limit access to Customer Data;
   iii. Restrict Ansys access to Customer Data to authorized employees with a demonstrated business purpose on a limited, as-needed basis; and
   iv. 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- Customer acknowledges and agrees that Ansys does not maintain physical data centers to support the Ansys Cloud Platform. Ansys leverages third-party providers to provide the Ansys Cloud Platform. Ansys conducts regular due diligence on its providers (which includes reviewing applicable industry standard reports and verifications of such providers) to assess whether the third-party providers have appropriate security controls addressing the security, integrity, and availability of the Ansys Cloud Platform. 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 Customer without undue delay. A notification required under this Section 9 shall be addressed to contact details as provided in the relevant ordering document, and 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. Audits and Assessments

a. Service Assessments- With respect to the Ansys Cloud Platform, Ansys shall:
   i. Periodically assess the Ansys Cloud Platform 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 Ansys Cloud Platform; and
   iii. Implement procedures to document and address vulnerability discovered during the testing outlined in 10(a)(i) and (ii).
b. Audit - Customer may request, no more than once per calendar year, evidence of Ansys' compliance with this Ansys Cloud Security Addendum. Notwithstanding anything herein to the contrary, such evidence of compliance shall be limited to Ansys completing a security questionnaire that would evaluate the technical and organizational security measures of the Platform.

11. Miscellaneous

a. Updates- Ansys may update this Cloud Security Addendum without notice to reflect the latest updates to the Ansys Security Program and the technical and organizational safeguards designed to secure the Ansys Cloud Platform, provided that such updates shall not result in a material degradation of the security of the Ansys Cloud Platform. The current version of the Cloud Security Addendum is available athttps://www.ansys.com/legal/agtc.