AVEVA GENERAL SUPPLIER CYBERSECURITY AND RESILIENCE TERMS AND CONDITIONS

Last Updated 13 April 2026

This Appendix between AVEVA and Supplier provides additional terms associated with security and cyber resilience provided by Supplier. It applies to any products, or services provided by Supplier that supports AVEVA's business operations which may involve access to AVEVA's systems, data or intellectual property.

In the event of a conflict, inconsistency or difference between this Appendix and other part of the Agreement, the terms of this Appendix shall control. Unless otherwise specified or the context warrants a different interpretation, the Agreement shall mean the Agreement between AVEVA and Supplier for the supply of products and/or services together with all applicable appendices, including this Appendix.

If the Supplier's role, access, or risk classification changes during the term of the Agreement, AVEVA reserves the right to require Supplier to comply with additional cybersecurity and resilience requirements applicable to higher risk categories.

1. General Obligations

Supplier shall implement and maintain reasonable and appropriate administrative, technical, and organisational measures to protect the security of its own systems and operations and to prevent unauthorised access, loss, theft, or misuse of any AVEVA data, information, or systems to which it may have limited access.

2. Acceptable Use and IT Hygiene

Supplier shall:

a. Use only authorised, properly licensed, and up-to-date software on all systems used to work for, access or process AVEVA information;
b. Maintain current operating system and application patch levels, applying security updates in a timely manner;
c. Implement basic access controls, including unique user accounts, password protection, and multi-factor authentication (MFA) where supported;
d. Ensure antivirus, endpoint protection, and firewall technologies are enabled, actively running, and kept up to date on all relevant devices; and
e. Ensure personnel receive periodic cybersecurity awareness training appropriate to their role, responsibilities, and level of exposure to AVEVA information or systems.

3. Confidentiality and Regulatory Compliance

Supplier shall keep all AVEVA information confidential and use it only for the purposes of providing the agreed products or services. Supplier shall not copy, transfer, or disclose AVEVA information except as expressly authorised in writing by AVEVA. Supplier shall comply with all applicable laws and regulations relating to privacy, data protection, confidentiality and cybersecurity, including (where applicable) use of AI.

4. Incident Notification

Supplier shall notify AVEVA of any known or suspected security incident that will have direct impact on AVEVA information, systems, or services as soon as reasonably practicable after discovery and provide sufficient information to allow AVEVA to assess potential impact via secure@aveva.com.

5. Best Practice

Where possible, Supplier shall demonstrate or align with recognised baseline security standards such as Cyber Essentials/Plus, ISO 27001, or equivalent industry best practice. Upon request by AVEVA, and subject to mutually agreed and reasonable confidentiality provisions, Supplier shall provide to AVEVA its current security policy.

6. Return of Asset

At any time during the term of the Agreement at AVEVA's request or upon the termination or expiration of the Agreement for any reason, Supplier shall, return to AVEVA for all AVEVA data or systems in its possession or the possession of any third parties.