AVEVA MEDIUM-RISK SUPPLIER CYBERSECURITY 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. These terms apply to any software, products and/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 software 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. **Standard of care**

   Where Supplier has access to AVEVA Systems including, but not limited to, mainframes, authorized endpoints, computers or devices, servers), owned, licensed, operated by, or used by AVEVA and/or AVEVA's customers in connection with the software and/or services ("**AVEVA Systems**") and/or collects, stores, or otherwise processes data from or on behalf of AVEVA (including without limitation data from AVEVA employees, prospects, customers, partners or users) in connection with the provision of the products or services including any data that may be generated by the provision of the products or services (**"AVEVA Data"**), Supplier shall at a minimum:

   a. only access, collect, store, or otherwise process AVEVA Data for the sole purpose of fulfilling the Supplier's obligations under the Agreement, or as otherwise expressly permitted by AVEVA in writing.

   b. maintain reasonable and appropriate administrative, technical, and organizational measures to preserve and protect the confidentiality, integrity, availability, and security of AVEVA Systems and AVEVA Data, aligned with applicable industry standards such as ISO27001, SOC2 Type II, NIST CSF and/or IEC 62443.

   c. should the technology, products and/or services contain any software, firmware, or chipsets; the development and productions of such must be demonstrably aligned with good industry practices and standards such as ISO27001, SOC2 Type II, NIST CSF and/or IEC 62443.

   d. ensure its employees and third parties receive annual cyber security related training and have current knowledge of cyber security best practices, relating to domains such as, but not limited to phishing, password/authentication protection and strength, information classification and sharing, security incidents report, etc. Upon request, Supplier shall provide evidence that any specific individual assigned to the

software and/or services under this Agreement, has successfully completed the required cybersecurity training within the past twelve (12) months.

e. implement appropriate personnel security and integrity procedures and practices, including but not limited to, conducting background checks consistent with applicable law.

f. not disclose, directly or indirectly, AVEVA Data to an unauthorized third-party, without express written consent from AVEVA unless and to the extent required by government authorities or as otherwise, to the extent expressly required, by applicable law.

g. comply with any other applicable security policies or procedures that AVEVA may provide or make available from time to time to Supplier as the context requires; especially when Supplier has access to AVEVA Systems and/or network, either at AVEVA location or remotely.

2. **Business Continuity:** Suppliers shall maintain business continuity and disaster recovery measures proportionate to the criticality of the products and services provided to AVEVA and taking into consideration AVEVA Systems and AVEVA Data, and cybersecurity risks must be included in its comprehensive risk analyses, contingency plan and solutions for its continuous delivery and operations.

3. **Security Incident Management:** In the event Supplier detects a confirmed or reasonably suspected misuse, compromise, or unauthorized access, destruction, loss, alteration, acquisition or disclosure of any AVEVA Data or AVEVA Systems, whether in Suppliers' IT systems or network, products and/or services, or otherwise in relation to the Supplier ("**Security Incident**"):

   a. Supplier shall notify AVEVA without undue delay and no later than the severity timelines set out below based on incident severity through AVEVA's Supplier Breach Notification Portal at: secure@aveva.com

Security Incident Severity	Definition	Initial Notification	Full Report
Critical	Major impact on operations, data breach affecting many individuals, or cross-border implications.	Within twenty-four (24) hours	Within five business day
High	Significant disruption or data breach with limited scope.	Within forty-eight (48) hours	Within five (5) business days
Medium	Moderate operational impact, no sensitive data breach.	Within seventy-two (72) hours	Within seven (7) business days
Low	Minor incidents, no data loss or service disruption.	Monthly summary	Quarterly report

b. Such notification shall contain at a minimum: (a) a brief description of the Security Incident, (b) any AVEVA Data or AVEVA Systems affected by the Security Incident, (c) any persons involved with the Security Incident, including any persons who made any unauthorized use or received an unauthorized disclosure, if known, (d) what Supplier has done or shall do to investigate the Security Incident, to mitigate any deleterious effects, and to protect against any further harm or other similar Security Incidents, and (e) any other information reasonably requested by AVEVA related to the Security Incident.

c. Supplier shall provide the name and contact details (including email address) of their designated security contact for the duration of this Agreement. This contact will serve as the primary point of communication for incident management and any security issues related to business continuity and resilience to AVEVA operations.

d. Take prompt steps to investigate, contain, and remediate any Security Incident and cooperate with AVEVA in any subsequent investigation and response in connection with Supplier's IT Systems or networks, or in relation with the software and/or services, and evidence demonstrating the completion of those activities. Unless otherwise specified hereto, each party will bear its own cost in relation to its performance and action contemplated as determined herein.

4. **Compliance with applicable laws:** Supplier shall, in performing its obligations under this Agreement, comply with all applicable laws, regulations, and industry standards relating to cybersecurity, data protection and information security, including those applicable in the jurisdictions in which the software and/or services are developed, hosted, or provided. In accordance with the European Union's NIS2 directive, AVEVA is required to implement appropriate cybersecurity risk management measures including measures addressing supply chain security. To enable AVEVA to meet these requirements, Supplier shall implement robust risk management practices, including regular vulnerability assessments and penetration testing, to ensure the security and resilience of its information systems and shall provide evidence of such compliance, including as may be applicable, summary of its technical documentation, vulnerability handling policy, classification, transparency, risk-management obligations or a written self-attestation confirming adherence.

5. **Vulnerability Management:** Supplier shall notify AVEVA of any actively exploited vulnerability identified in any software and/or services provided under this Agreement, according to the below requirements:

   a. Supplier shall fully cooperate with AVEVA in assessing the impact of the vulnerability, by providing timely updates as new information becomes available and supporting AVEVA in communicating with affected stakeholders, regulators, or authorities as may be applicable.

b. Supplier shall maintain detailed records of all vulnerabilities, notifications, and remediation actions for a minimum of five (5) years and shall make such records available to AVEVA upon request for audit or compliance verification purposes.

c. Supplier shall align its vulnerability management process with recognised standards such as ISO/IEC29147, ISO/IEC 30111, or equivalent, and where applicable with the principles of the EU Cyber Resilience Act (CRA) and, if applicable, Supplier shall comply with its vulnerability reporting obligations to relevant national authorities as required by the CRA, and upon AVEVA's request, Supplier shall provide confirmation of such compliance and relevant documentation regarding its CRA vulnerability handling procedures.

d. Supplier shall take immediate actions to mitigate and remediate such issues that are consistent with the requirements and obligations set forth in the below table:

Severity	Corrective patch/remediation (from date of discovery)	Notification to AVEVA
Critical (1) CVSS 9.0 - 10.0	Seven (7) days	24 hours of discovery
High (2) CVSS 7.0 - 8.9	Fourteen (14) days	48 hours of discovery
Medium (3) CVSS 4.0 - 6.9	Sixty (60) days	3 business days of discovery
Low (4) CVSS 0.1 - 3.9	Ninety (90) days	All unpatched vulnerabilities due to supplier's business operation or technical issues after 90 days

e. In the event of any deviations with corrective patch availability mentioned above, Supplier shall provide a reasonable justification approved by AVEVA in writing.

f. Supplier acknowledges that AVEVA may utilize external platforms to conduct non-intrusive monitoring on an ongoing basis. In the event that, any of these platforms identify issues, particularly those related to web applications, TLS/SSL configurations and certificates, Botnet Infections, SPF Domain misconfiguration, and DMARC, etc., AVEVA security risk assessor shall ask the supplier to remediate such issues as part of the ongoing engagement.

6. Audit and assessment

a. AVEVA shall have the right to audit Supplier once every twelve (12) months, to evaluate Supplier's compliance with this Appendix, as well as industry standards. To that purpose, Supplier shall share an executive report of such audit, to the extent such audit covers the scope of the software and/or services. If Supplier does not conduct

its own audit, Supplier grants AVEVA or, upon AVEVA's election, a mutually agreeable third party on AVEVA's behalf, permission to perform an assessment In the event of any issues or findings, Supplier shall remediate any issues and/or findings, at its sole cost and expense, and within a reasonable time as agreed upon in writing by both parties.

b. Additionally, upon request from AVEVA, Supplier will provide its own current penetration test report within the last 12 months or executive summary to AVEVA to the extent such penetration test covers the scope of the software and/or services, subject to appropriate confidentiality protections. Supplier may redact information from such summary where disclosure could compromise Supplier's security posture, provided that Supplier shall not redact findings material to AVEVA's risk assessment

7. **Updates**
   Supplier shall provide support and security updates including vulnerability resolution for product lifecycle or service, consistent with industry best practices and applicable laws. Supplier shall notify AVEVA in writing at least twelve (12) months prior to discontinuation of any product or service and offer reasonable assistance during the transition period
8. **Configuration guidelines:** Supplier commits to provide secure configuration guidelines that fully describe all security-related configuration options and their implications for the overall security of the software and/or services. The guidelines shall include, without limitation, a full description of any dependencies on the supporting operating system, how they should be configured for optimal security, and how the default configuration of the products and/or services shall be secure. Supplier is responsible for releasing patches, updates, and fixes to address cybersecurity vulnerabilities in the products and/or services (e.g., OS, firmware, specific solution).

9. **AI Systems:** Where Supplier uses, deploys, or incorporates artificial intelligence (including machine learning, generative AI, or automated decision-making systems) in the provision of products or services under this Agreement ("AI Systems"), Supplier shall ensure that any AI systems used under this Agreement:
   a. comply with applicable laws and regulations including the EU AI Act (where relevant) and relevant industry standards such as ISO/IEC 23053 and 42001.
   b. (i) process AVEVA Data for the purpose of performing its obligations under this Agreement; (ii) not use AVEVA Data to train, fine-tune, or improve any AI models, whether for Supplier's own benefit or for third parties, without AVEVA's prior written consent (iii) do not use AVEVA Data as input for generative AI Systems except where expressly authorised by AVEVA and subject to appropriate agreed safeguards .
   c. upon AVEVA's reasonable request, provide documentation regarding AI Systems used in connection with this Agreement, including (i) a description of the AI System's intended purpose and functionality; (ii) known limitations, risks, and potential for bias or error (iii) data sources and provenance used to train or operate the AI System (iv) any third-party AI services or models integrated into the AI System.

d. do not make or support decisions that affect AVEVA, its employees, or AVEVA Data with no human oversight, without AVEVA's prior consent
e. notify AVEVA of any material changes in writing at least 30 days in advance that could materially affect functionality, compliance, security or risk profile.
f. permit audits to verify adherence to these obligations.

10. Return or destruction of data

a. Upon the termination or expiration of the Agreement, Supplier shall within 30 days return to AVEVA all copies, whether in written, electronic or other form or media, of AVEVA Data in its possession or the possession of its third parties, or at AVEVA 's option, securely dispose of all such copies, and certify in writing to AVEVA that such AVEVA Data has been returned to AVEVA or disposed of securely.
b. 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 all AVEVA Systems in its possession or the possession of any third parties.
c. 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, and shall instruct all third parties to, disconnect any and all interfaces and connections to AVEVA Systems and, upon AVEVA's request, shall provide evidence of such disconnection.