



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

Last Updated 30 April 2026

This Appendix between AVEVA and Supplier provides additional terms regarding security and cyber resilience provided by Supplier. These terms apply to all Suppliers providing Information Technology and related professional services to AVEVA, including (without limitation) delivery of software, hardware, cloud hosted services and platforms, managed services and outsourced IT functions and AI enabled solutions.

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 together with all applicable appendices, including this Appendix.

This Appendix may be reviewed and amended by AVEVA upon contract renewal or in the event of a material change in the scope of software and/or services. Supplier agrees to engage in good faith discussions to incorporate such updates.

1. Definitions

In this Appendix, the following terms shall have the meanings set forth below. Any capitalized terms that are used in this Appendix but not defined herein will have the same meanings as set forth in the Agreement.

"Affiliates" with respect to either party, an "Affiliate" shall mean any entity that directly or indirectly Controls, is Controlled by, or is under common Control with, another entity.

"Applicable Industry Standards" as part of this Agreement, it has been defined that the following standards will apply: ISO27001:2022, SOC2 Type II, NIST CSF 2.0, ISA/IEC 62443 - 4 -1, NIST SP 800-218.

"AVEVA" means AVEVA or any of AVEVA's Affiliate(s) as the context requires.

"AVEVA Users" means any of AVEVA's customer(s) or end user(s) of AVEVA's products, equipment, or services, to which or at which the Software and/or Services of the Supplier are provided, used, or integrated

"AVEVA Data" means all information, content, and data, including, without limitation, all text, sound, software, files, or Personal Data that are provided to Supplier by AVEVA and/or AVEVA Users in connection with the Software and/or Services. AVEVA Data may include information, content, and data that AVEVA and/or AVEVA Users (i) input to the Software and/or Services; and/or (ii) create and/or modify using the Software and/or Services

"AVEVA Systems" means all systems (including but not limited to mainframes, authorized endpoints, computers or devices, servers), owned, licensed, operated by, or used by AVEVA and/or AVEVA Users in connection with the Software and/or Services

"Authorized Employees" means Supplier's employees or employees of its Affiliates who have a need to know or otherwise access AVEVA Systems and/or AVEVA Data to enable Supplier to perform its obligations under the Agreement.

"Authorized Persons" means (i) Authorized Employees; and (ii) Supplier's contractors, agents, outsourcers, and auditors who have a need to know or otherwise access AVEVA Systems and/or AVEVA Data to enable Supplier to perform its obligations under the Agreement, and who are bound by confidentiality obligations sufficient to protect AVEVA Systems and/or AVEVA Data as provided in the Agreement.

AVEVA High-Risk Supplier Cybersecurity Terms And Conditions v1 (30 April 2026)



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

“Confirmed” means verified or established as true or valid based on sufficient evidence or investigation.

“Containment” or **“Contain”** means to stop the spread or further damage caused by a Security Incident. The Vulnerability or underlying issue may still exist, but it no longer poses an immediate Threat.

“Control” means, in respect of any entity, the possession, directly or indirectly, of the power to direct or cause the direction of the management of such entity, whether through the ownership of voting securities (or other ownership interest), by contract or otherwise

“Penetration Test” means an authorized simulated cyberattack on Supplier Information Systems, using real-world exploits and techniques within pre-defined limits or ‘rules of engagement’ performed to evaluate the security of such a system. The test is performed to identify weaknesses (also referred to as ‘Vulnerabilities’), including the potential for unauthorized parties to gain access to Supplier Information Systems features and data, to enable a full risk assessment to be completed.

“Personal Data” means information relating to an identified or identifiable natural person (“Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

“Reasonably Suspected” means a belief or assumption that an event or condition may have occurred, based on credible information or observable indicators, even if not yet confirmed through full investigation.

“Remediation” means the Security Incident has been analyzed and Contained, the Threat has been neutralized, and changes have been made to prevent a recurrence of the same incident.

“Resilience” means the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

“Supplier Information Systems” are any hardware, software, or other information assets used by Supplier to deliver, provide, or support the Software and/or Services for AVEVA, including but not limited to laptops, servers, mobile computing devices, cloud infrastructure, and any associated software applications.

“Security Incident” means a Confirmed or Reasonably Suspected occurrence that (i) actually jeopardizes the confidentiality, integrity, security or availability of any, AVEVA Data, Supplier Information Systems, AVEVA Systems or any information processed, stored or transmitted on them; and/or (ii) disrupts AVEVA’s or AVEVA Users operation; and/or (iii) violates applicable cybersecurity, information security and/or personal data laws or regulations associated with the delivery of Software and/or Services and Applicable Industry Standards as defined above.

“Secure Development Lifecycle” or **“SDL”** means a process that standardizes security best practices for designing, implementing, testing and maintaining development across a range of products and services by embedding security into the product or application development process including requirements, design, coding, testing, and extending the best practices into the operation, and maintenance and eventual removal of the product and the system and a process conforming with the requirements of Microsoft SDL, NIST Secure Software Development Framework (SSDF) or an industry standard equivalent.



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

“Software and/or Services” means the technology products and services such as software, hardware, cloud hosted services and platforms, managed services, outsourced IT functions, AI enabled solutions and other related services or products provided to AVEVA by the Supplier under the Agreement.

“Technical and Organizational Security Measures” means security measures used to protect Supplier Information Systems and, by extension, AVEVA Systems and/or AVEVA Data that (i) are appropriate for the types of AVEVA Systems, AVEVA Data that are associated with the delivery of the Software and/or Services, (ii) include reasonable and appropriate administrative, operational, technical, physical and organizational measures and safeguards that (a) are consistent with industry standards and applicable laws and (b) are designed to protect AVEVA Systems and AVEVA Data against any Security Incident, and protect the security, integrity and confidentiality of AVEVA Data, (iii) comply with industry standard security requirements, obligations, specifications or event reporting procedures associated with the delivery of Software and/or Services identified and agreed by both parties as appropriate for the delivery of Software and/or Services as set forth below. As part of such security measures, Supplier shall provide a reasonably secure environment for all AVEVA Systems and AVEVA Data provided to or used by Supplier as part of its performance associated with the delivery of Software and/or Services.

“Threat” means any risk that could potentially compromise the integrity, availability or confidentiality of the system, data, or commands of the control and safety systems or components.

“Vulnerability” means a weakness within a Software and/or Service that allows an unauthorized reduction of the Software and/or Services information assurance level. Vulnerabilities can be exploited by a Threat source to perform unauthorized actions within the Software and/or Services.

2. Standard of Care

Where Supplier has access to AVEVA Systems and/or 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 security 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. 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 Authorised Persons has successfully completed the required cybersecurity training within the past twelve (12) months.
- d. not disclose, directly or indirectly AVEVA Data to an unauthorized third-party, without express written consent from AVEVA
- e. comply with applicable security policies or procedures that AVEVA may provide or make available from time to time to Supplier as the context requires



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

- f. If the technology, products and/or services provided contain any software, firmware, or chipsets, Supplier shall ensure 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.
- g. Suppliers shall maintain business continuity and disaster recovery measures proportionate to the criticality of the Software and/or Services to ensure its continued provision under this Agreement.
- h. Supplier shall be responsible for and remain liable to AVEVA for the actions and omissions of all Authorized Persons concerning the treatment of AVEVA Systems and AVEVA Data as if they were Supplier's own actions and omissions.
- i. 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 Supplier Information Systems.
- j. 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. Upon AVEVA's reasonable request, Supplier shall provide evidence of such compliance, including as may be applicable, summary of its technical documentation, certifications, vulnerability handling policy, classification, transparency, risk-management obligations or a written self-attestation confirming adherence. Supplier shall promptly notify AVEVA of any material non-compliance or regulatory investigation relating to the Software and/or Services that could reasonably impact AVEVA Systems or AVEVA Data.
- k. AVEVA Systems and AVEVA Data are deemed to be Confidential Information of AVEVA and are not Confidential Information of Supplier.
- l. To ensure the highest levels of security and operational efficiency, it is essential to prevent the usage and procurement of obsolete software. Supplier must conduct regular reviews of its software inventory to identify and phase out any outdated or unsupported software applications. This includes ensuring that all software in use is actively maintained, receives regular security updates, and complies with current industry standards. Procurement processes should include stringent criteria to evaluate the longevity and support lifecycle of software products, prioritizing those with robust support and update policies. Avoiding obsolete software mitigates security risks, enhances system performance, and ensures compliance with regulatory requirements. Upon reasonable request, Supplier shall provide appropriate evidence of compliance with this requirement.

3. Information Security

- a. Supplier shall implement Technical and Organizational Security Measures with respect to any AVEVA Systems it utilizes in connection with the Software and/or Services and to protect any AVEVA Data it processes in connection with the Agreement. Such Technical and Organizational Security Measures



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

shall be no less rigorous than the Applicable Industry Standards. At a minimum, Supplier's Technical and Organizational Security Measures shall include, but are not limited to:

- i. limiting access of AVEVA Systems and/or AVEVA Data to Authorized Persons or Supplier Information Systems;
 - ii. securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;
 - iii. implementing network, device application, database, and platform security;
 - iv. securing information transmission, storage, and disposal;
 - v. implementing authentication and access controls within media, applications, operating systems, and equipment;
 - vi. encrypting AVEVA Data at rest and AVEVA Data transmitted over public or wireless networks;
 - vii. strictly segregating (electronically and/or physically) AVEVA Systems and/or AVEVA Data from information of Supplier or its other customers or suppliers; and
 - viii. implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law.
- b. Supplier represents and warrants that the Software and/or Services do not contain any known Vulnerabilities or malware and have been scanned using industry-standard practices to detect and prevent malicious code, including viruses, backdoors, and other harmful code. Supplier shall regularly monitor its information systems for potential Threats, conduct Vulnerability scans, and perform penetration testing. This includes ensuring that all downloadable documents are free from malicious code by implementing rigorous security measures such as regular audits and up-to-date antivirus and anti-malware software. By providing Software and/or Services to AVEVA, Supplier acknowledges and agrees to these security requirements, accepts full responsibility for any breach, and recognizes AVEVA's right to conduct independent security assessments and take appropriate action in cases of non-compliance.
- c. In alignment with industry best practices and regulatory standards, Supplier shall integrate Secure Development Lifecycle (SDL) principles into its software development processes. This involves incorporating security at every stage of the development lifecycle, from initial design through to deployment and maintenance. Key SDL practices include Threat modeling, secure coding standards, regular code reviews, and security testing such as static and dynamic analysis. Additionally, Supplier shall ensure that all development personnel receive ongoing training in secure development practices. Embedding SDL requirements into the development process, ensures that software products are resilient against Vulnerabilities and Threats, thereby protecting AVEVA Systems and AVEVA Data from potential Security Incidents.



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

- d. To effectively manage and mitigate risks associated with zero-day Vulnerabilities, it is essential to maintain a comprehensive Software Bill of Materials (SBOM) for all software products and platforms used by AVEVA. SBOM requirements include but are not limited to
- e. Component Inventory: Supplier must maintain an up-to-date SBOM that lists all software components, including open-source libraries, third-party dependencies, and proprietary code. Each entry should include the component name, version, license information, and source.
- f. Vulnerability Tracking: Supplier must implement processes to continuously monitor and track Vulnerabilities associated with components listed in the SBOM. This includes subscribing to relevant Vulnerability databases and security advisories.
- g. Impact Assessment: Upon discovery of a zero-day Vulnerability, Supplier must promptly assess the impact on its products and platforms by cross-referencing the SBOM. This assessment should identify which products or internal software are affected and the severity of the impact.
- h. Remediation Plan: Supplier must develop and implement a remediation plan for addressing Vulnerabilities identified through the SBOM. This plan should include timelines for patching or updating affected components, testing procedures, and communication protocols for informing stakeholders.
- i. Regular Updates: The SBOM must be regularly updated to reflect changes in the software components, including additions, removals, and version updates. Supplier should establish a schedule for periodic reviews and updates of the SBOM.
- j. Transparency and Sharing: Supplier must ensure that the SBOM is accessible to relevant stakeholders, including AVEVA (on reasonable request and subject to reasonable confidentiality obligations), to facilitate transparency and collaboration in Vulnerability management. This includes providing SBOM details upon request and during security assessments.
- k. If the provision of the Software and/or Services under the Agreement includes interaction with payment card information or systems by Supplier or Supplier Information System, Supplier shall at all times be PCI DSS certified, or if not certified provide sufficient evidence of compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Supplier's sole cost and expense.
- l. During the term of each Authorized Employee's employment by Supplier and Authorized Persons engaged by Supplier under the Agreement, Supplier shall at all times cause such Authorized Employees and Authorized Persons to abide strictly by Supplier's obligations under the Agreement, and Supplier's standard policies and procedures. Supplier further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of AVEVA Systems and/or AVEVA Data by any Authorized Persons or any of Supplier's officers, partners, principals, employees, agents, or contractors.



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

- m. Supplier shall be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of AVEVA Systems and AVEVA Data under its control or in its possession.
- n. Supplier shall ensure that the Software and/or Services provided to AVEVA are certified to meet the requirements of Applicable Industry Standards, and by extension, the requirements of AVEVA’s technical security requirements standard, as may be provided to Supplier prior to the Agreement.
 - i. Upon request from AVEVA, Supplier shall provide documentation demonstrating the compliance of the Software and/or Services with Applicable Industry Standards.
 - ii. In the event of non-compliance and/or Vulnerabilities, whether detected through non-intrusive monitoring such as external platforms or other means, Supplier shall take immediate actions to mitigate and remediate such issues that are consistent with the requirements and obligations set forth in this Appendix.
 - iii. AVEVA reserves the right to verify Supplier’s compliance with the requirements outlined in this clause at regular intervals, with reasonable written notice. Supplier shall reasonably cooperate with such requests and provide reasonable access and information to verify compliance.
- o. Supplier acknowledges that its employees, contractors, and agents may only utilize devices either owned by AVEVA or owned and/or managed by Supplier in the provision of the Software and/or Services to AVEVA under the Agreement. For the avoidance of doubt, Supplier, and Supplier’s employees, contractors, or agents, are not permitted to use any Bring Your Own Device(s) (“BYOD”) in the provision of the Software and/or Services under the Agreement to AVEVA, unless those devices are centrally managed by Supplier and maintain the same or more restrictive cybersecurity controls as Supplier-issued devices.

4. Security Incident Management

- a. In the event Supplier detects a Confirmed or Reasonably Suspected Security Incident, Supplier shall notify AVEVA following below timelines based on Security Incident severity through AVEVA’s Supplier Breach Notification Portal at: secure@aveva.com (including incident details and sender’s full name, email, phone number, country, and organization name)

| 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 seventy-two (72) hours |
| High | Significant disruption or data breach with limited scope. | Within forty-eight (48) hours | Within five (5) business days |

AVEVA High-Risk Supplier Cybersecurity Terms And Conditions v1 (30 April 2026)



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

| | | | |
|---------------|--|-------------------------------|--------------------------------|
| 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. Supplier shall take prompt steps to investigate, contain, and remediate any Security Incident and cooperate with AVEVA in any subsequent investigation and response in connection with Suppliers Information Systems, or in relation with the Software and/or Services, and evidence demonstrating the completion of those activities.
- e. Supplier agrees that it shall not, unless otherwise required by law, inform any third party of the AVEVA specific aspects of any Security Incident (including without limitation mentioning AVEVA or AVEVA Users by name) without first obtaining AVEVA's prior written consent, other than to inform a complainant that the matter has been forwarded to AVEVA's appropriate person. Further, with regard to notice that AVEVA may issue related to the Security Incident, Supplier agrees that AVEVA shall have the sole discretion to determine:
 - i. whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in AVEVA's discretion; and
 - ii. the contents of such notice, whether any type of Remediation may be offered to affected persons, and the nature and extent of any such Remediation.
- f. Supplier agrees to cooperate at its own expense with AVEVA in any litigation or other formal action which may be necessary to protect AVEVA's rights relating to the use, disclosure, protection and maintenance of AVEVA Systems and AVEVA Data.

5. Audit and Security Assessments



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

- a. Without limiting other audit rights that AVEVA may have under the Agreement, AVEVA shall have the right to audit Supplier once every twelve (12) months, to evaluate Supplier's compliance with this Appendix, as well as the Applicable Industry Standards. To that purpose, Supplier grants AVEVA or, upon AVEVA's election, a mutually agreeable third party on AVEVA's behalf, permission to perform an assessment including supporting documentation validation of all controls in Supplier's physical and/or technical environment in relation to all AVEVA Systems and/or AVEVA Data being handled or accessed by Supplier and/or the Software and/or Services being provided to AVEVA pursuant to the Agreement (each, a "Security Assessment"). Upon reasonable advance notice, Supplier shall fully cooperate with such Security Assessment by providing access to knowledgeable personnel, physical premises, documentation, and Supplier Information Systems. If Supplier conducts its own Security Assessments outside AVEVA's audit rights specified herein, in AVEVA's sole discretion, Supplier may share an executive report of such Security Assessment with AVEVA once annually upon request in lieu of AVEVA's right to audit herein to the extent such Security Assessment materially complies with the requirements of this section and covers the scope of the Software and/or Services being delivered to AVEVA. Additionally, upon request from AVEVA, Supplier will provide its own current Penetration Test report within the last 12 month 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 Supplier shall not redact findings material to AVEVA's risk assessment.
- b. In the event of a Security Incident, AVEVA may require Supplier to provide a copy of the audit report generated by a third party which is generally accepted by industry as professional in such type of audit and engaged by Supplier to conduct a Security Assessment after the Security Incident.
- c. The party conducting the Security Assessment shall share the full and unredacted results of such Security Assessment with the other party which shall treat such information as Confidential Information. Supplier shall Remediate any issues and/or findings identified in a Security Assessment at the sole cost and expense of Supplier and within a period of no more than sixty (60) days unless otherwise agreed upon in writing by both parties. Unless otherwise specified hereto, each party will bear its own cost in relation to its performance and action contemplated as determined in this Appendix.

6. AI Systems

Where Supplier uses, deploys, or incorporates artificial intelligence (including machine learning, generative AI, or automated decision-making systems) in the provision of Software and/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;



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

- b. (i) process AVEVA Data only for the purposes set out under this Agreement; (ii) do 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; and
- f. permit audits to verify adherence to these obligations.

7. Vulnerability Management & Response

- a. Supplier shall align its vulnerability management process with recognised standards such as ISO/IEC29147, ISO/IEC 30111, or equivalent. Where Supplier software falls within scope of the EU Cyber Resilience Act (CRA), Supplier shall comply with its vulnerability reporting obligations to relevant national authorities as required by the CRA. Upon AVEVA's request, Supplier shall provide confirmation of such compliance and relevant documentation regarding its CRA vulnerability handling procedures. 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.
- b. Supplier shall notify and take immediate actions to mitigate and remediate identified Vulnerability in their Software and/or Service that could impact AVEVA, including actively exploited Vulnerabilities. The severity level of a Vulnerability shall be analyzed and scored using the then-latest version of the Common Vulnerability Scoring System (CVSS) or an equivalent standard 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 to Fourteen (14) days | 24 hours of discovery |



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

| | | |
|------------------------------|-----------------------------------|--|
| High (2) CVSS 7.0 - 8.9 | Thirty (30) days | 48 hours of discovery |
| Medium (3) CVSS 4.0 - 6.9 | Sixty (60) to Ninety (90) days | 3 business days of discovery |
| Low (4) CVSS 0.1 - 3.9 | One Hundred and Eighty (180) days | All unpatched vulnerabilities due to supplier's business operation or technical issues after 90 days |

8. Vulnerability Tracking and Recording

- a. Supplier will track and record all Vulnerabilities uncovered during the entire lifecycle of the Software and/or Services, including whether the Vulnerability is a requirement, design, implementation, testing, deployment, or operational issue.
- b. Supplier shall develop and implement an "Action Plan" which shall include policies and procedures to address Vulnerabilities. The Action Plan includes identifying all affected versions, root cause, how the issue will be resolved, and the expected resolution date. The Action Plan shall include appropriate provisions for mitigating the harmful effects of the Vulnerability and addressing and remedying the occurrence(s) to prevent the recurrence of similar Vulnerabilities in the future. The development and implementation of the Action Plan shall follow industry standard practices, such as those that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61, and NIST Special Publication 800-53.
- c. Supplier shall provide recommendations to AVEVA on actions that AVEVA may take to assist in the prevention of recurrence, as applicable or appropriate.
- d. Following Vulnerability discovery, Supplier shall provide AVEVA with an Action Plan and corresponding corrective patch within a timeframe proportionate to the identified vulnerability's severity and risk impact and shall promptly implement the agreed measures without undue delay.
- e. 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.

9. Vulnerability Communication

- a. Supplier shall exercise due diligence and caution in preventing the public disclosure of information regarding Vulnerabilities to limit the likelihood that any Vulnerabilities in deployed / operational



AVEVA HIGH-RISK SUPPLIER CYBERSECURITY TERMS AND CONDITIONS

AVEVA Software and/or Services are exposed before a distributed fix is available. Supplier shall obtain AVEVA's approval before disseminating any disclosures that relate to AVEVA.

- b. Whether or not publicly disclosed by Supplier and notwithstanding any other limitation in this Appendix, AVEVA may disclose any Vulnerabilities, material defects, and/or other findings related to the Software and/or Services provided by Supplier to (a) an industry information sharing organization, (b) a Cyber Emergency Response Team ("CERT"), or any equivalent governmental entity or program, or (c) any entity required by applicable law.

10. Return or Destruction of AVEVA Data

- a. Upon the termination or expiration of the Agreement, Supplier shall within 30 days promptly 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, and shall instruct all Authorized Persons to, promptly return to AVEVA all AVEVA Systems in its possession or the possession of such Authorized Persons.
- 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 Authorized Persons to, disconnect any and all interfaces and connections to AVEVA Systems and, upon AVEVA's request, shall provide evidence of such disconnection.