TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The relevant technical and organisational measures taken by AVEVA to protect Personal Data include:

- Pseudonymisation and encryption of Personal Data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the Processing
- User identification and authorisation
- Protection of Personal Data during transmission and at rest
- Protection of physical security of locations at which Personal Data are Processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Certification/assurance of Processes and Products
- Measures to ensure data minimisation, data quality, limited data retention, accountability and data portability

In particular, AVEVA shall exercise reasonable efforts to implement the following measures in connection with information security of Customer Personal Data:

a) backing-up the Customer Personal Data at regular intervals;
b) ensuring that AVEVA is able, to restore lost or damaged Customer Personal Data from the latest back-up;
c) not using the Customer Personal Data except as required for the performance of its obligations under the Agreement;
d) upon Customer's written request, grant Customer access to current ISO 27001 certificate and annual AICPA SOC 2 Type II report;
e) complying with information management procedures and safeguards based on Good Industry Practice, i.e. ensuring the degree of skill, care and prudence (including that concerning the security of Customer Personal Data) which would ordinarily be expected of a skilled and experienced supplier of software products and services of the same or a similar nature to the Products, Services and Support Services of AVEVA;
f) maintaining and enforcing safeguards against the destruction, loss, or alteration of Customer Personal Data that are no less rigorous than those maintained by AVEVA for its own information of a similar nature or that otherwise comply with Good Industry Practice;
g) in the event of any destruction, loss, or reduction in the accessibility or usability of Customer Personal Data which is caused by AVEVA, restoring such data using Good Industry Practice data restoration techniques;
h) taking all necessary precautions, in accordance with Good Industry Practice, to prevent any Malicious Code (as defined in the AVEVA General Terms and Conditions and any applicable Addenda) affecting the Products or Services and the Customer Personal Data, including but not limited to using the latest versions of anti-malware software (including latest definitions and updates) available from an industry accepted anti-malware software vendor to check for and delete Malicious Code;
i) notifying the Customer as soon as practicable upon becoming aware of any Personal Data Breach and providing the Customer with a detailed description, the type of Customer Personal Data involved, the identity of any affected individuals and all other information and cooperation which the Customer may reasonably request;
j) taking immediate action, at AVEVA's own cost, to investigate any Personal Data Breach, to identify, prevent and mitigate the effects of such Personal Data Breach and, with the Customer's prior agreement, to carry out any recovery or other action necessary to remedy the Personal Data Breach. AVEVA must ensure that any such recovery or other action does not compromise any technical information or artefacts (including, for example, logs) which would reasonably be required by the Customer to understand the Personal Data Breach, mitigate its effects and/or prevent its recurrence;
k) not issuing, publishing or otherwise making available to any third party any press release or other communication concerning a Personal Data Breach without the Customer's prior approval (such approval not to be unreasonably withheld or delayed), unless communication is required by Applicable Data Protection Legislation or by any court or other authority of competent jurisdiction provided that before making such communication AVEVA to the extent lawful provides notice to the Customer that it will be making such communication and such communication must not reference the Customer (unless legally required to do so);

l) use of data centres where Customer Personal Data is stored, accessed or otherwise Processed, in accordance with Good Industry Practice;
m) keeping any Customer Personal Data in electronic form logically separated from any information, data or material of any third party;
n) ensuring that access to Customer Personal Data by AVEVA's personnel is restricted on a strictly need to know basis and that all AVEVA's personnel who are granted such access have completed appropriate security training in line with the AVEVA Group Data Protection Policy; and
o) performing service improvement and monitoring of the provision of the Products and Services and promptly rectifying any security vulnerabilities identified by such testing.

For further information on how we safeguard Customer Personal Data, please refer to AVEVA's Cloud Security Statement at https://www.aveva.com/en/legal/trust/security/, where you may also download AVEVA's whitepaper on cloud security.