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.

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 27001:2013 certificate and annual SAE18 SOC 2/ISAE3402 SOC (Type II) reports in respect of specific Software supplied under the Agreement (where stated to be available for that Software in the applicable Transaction Document or Software Schedule) addressing data security requirements stated in the Data Processing Addendum;
e) complying with information management procedures and safeguards based on Good Industry Practice, including those concerning the security of the Customer Personal Data. For the purpose of the Data Processing Addendum, "Good Industry Practice" means that degree of skill, care and prudence 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;
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 Software and Support Addendum) 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 Security Incident and providing the Customer with a detailed description of the Security Incident, the type of Customer Personal Data that is the subject of the Security Incident, the identity of any affected individuals and all other information and cooperation which the Customer may reasonably request. For the purpose of the Data Processing Addendum, "Security Incident" shall mean any incident resulting in loss, destruction or material alteration of Customer Personal Data, or unauthorized third-party access to Customer Personal Data;
j) taking immediate action, at AVEVA's own cost, to investigate any Security Incident, to identify, prevent and mitigate the effects of such Security Incident and, with the Customer's prior agreement, to carry out any recovery or other action necessary to remedy the Security Incident. 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 Security Incident, 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 Security Incident without the Customer's prior approval (such approval not to be unreasonably withheld or delayed), unless communication is required by Applicable DP 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 the Products, Services and 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 Privacy policy; and
o) performing continuous service improvement and continuous monitoring of the Services used in connection with the provision of the Products and Services and promptly rectifying any security vulnerabilities identified by such testing.

_____