Cybersecurity Checklist for Your Vendor

When it comes to cybersecurity, who you partner with is crucial. Software vendors play an important part in your cyber defence strategy. When considering a cloud or IIoT partner here are some key questions to consider.

Please use the check box ☐ below

Physical Security

- ☐ Where are their cloud services physically deployed?
- ☐ Where will my data actually reside?
- ☐ Where and how will my data be captured, stored and used?

Data Security

- ☐ How is your information protected – at rest and in motion?
- ☐ Does your vendor support unidirectional data transfer?
- ☐ How does your supplier deal with network outages?

Application Security

- ☐ How do they handle authentication, authorisation and account management?
- ☐ What is their approach to identity and access management (IAM)?
- ☐ Do you offer a flexible, scalable solution?

Continuous Monitoring

- ☐ Do they have proactive monitoring and active security policies in place?
- ☐ Can they identify abnormal behavior and catch anomalous activity?
- ☐ What procedures are there to detect and isolate suspicious activity online?

Security Assessments

- ☐ Do they have a proactive program of external security audits?
- ☐ How do they deal with ongoing compliance with regulations e.g. GDPR?
- ☐ Do you have a published security statement that I can read?

Projects and Delivery

- ☐ Are their delivery teams certified to global standards such as CMMi Level 5, ISO 9001?
- ☐ Do they have a Computer Security Incident Response Team (CSIRT) ready to mobilise?
- ☐ Do they have partnerships with key security experts e.g. Cylance, Claroty?

At AVEVA we are dedicated to earning and retaining your digital trust.

View our security statement at:
trust.aveva.com

Start your digital transformation today
connect.aveva.com/insight