Cybersecurity, Data Protection and Privacy at AVEVA

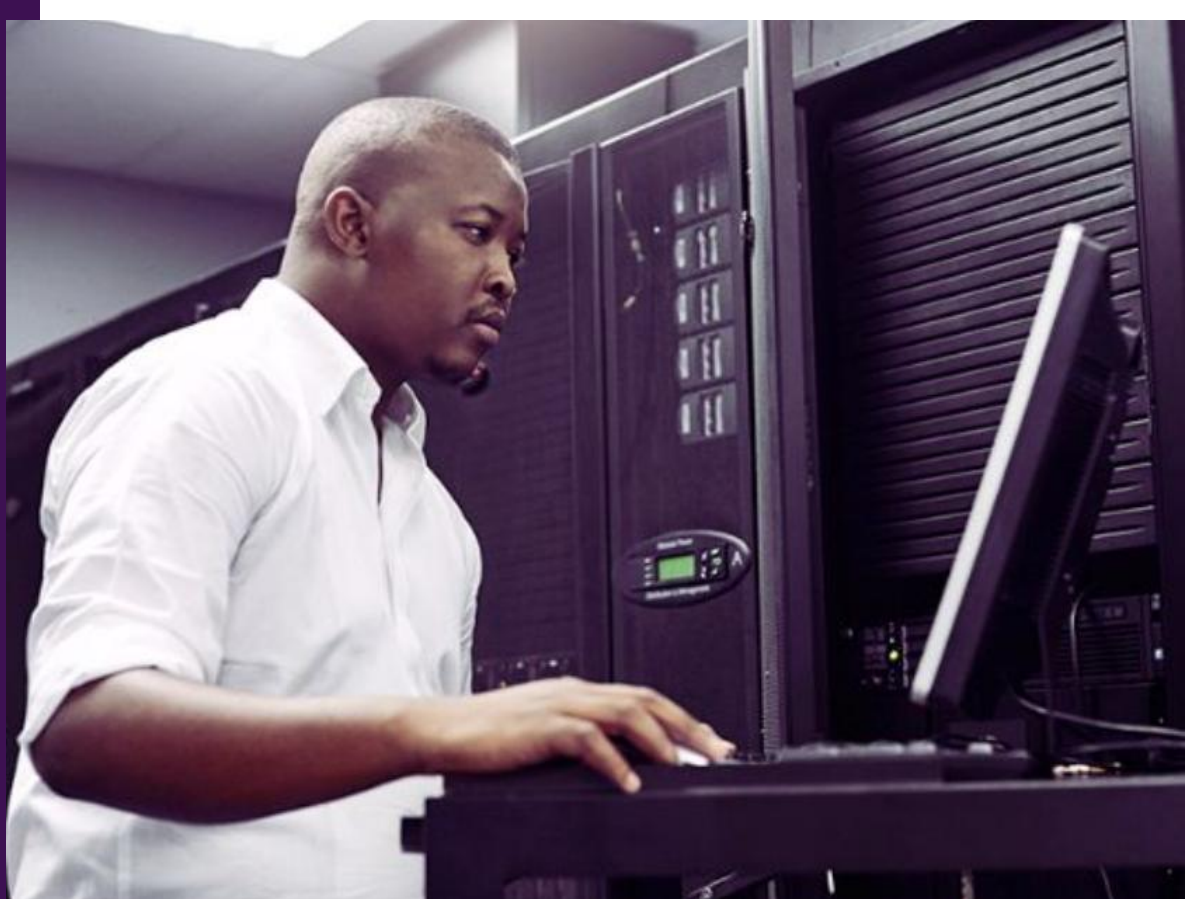
AVEVA is a global company, developing and delivering industrial software solutions purpose-built for the energy infrastructure and manufacturing sectors, whilst driving sustainable change for a sustainable future.

This document outlines the ways in which AVEVA ensures the security of its software, information and customer details, as well as how it mitigates related risks.

Contents

1. Introduction

Cybersecurity at AVEVA is an essential part of our business strategy to connect people with trusted information and insights to drive responsible use of world's resources. We understand the need of our customers to have critical services, systems and products built secure by design, default and deployment. We continuously improve our services, systems and products so they are secure-by-design and deployment, and we have resilient processes in place to protect our customers and business operations. This has allowed us to remain in the top 25% of software development businesses for external security performance benchmarking.



2. AVEVA Employees and Cybersecurity ISO

All AVEVA employees are required to complete mandatory annual cybersecurity compliance training. This training enables employees to fulfil their role and keep company and client data safe. The training covers procedures that employees must follow to prevent a range of different cybersecurity attacks including phishing, password theft and malware.

In 2024, more than 99% of our colleagues completed mandatory cybersecurity training. Exception cases are routed to employee supervisors for coaching, including emphasis on successful completion as a component of our reward package.

In addition to this mandatory training, we also provide role-based programs to advance security skills for employees who are known to face important cyber risks in their day-to-day work. Program activities range from curated lessons to engagements with industry experts, as well as support for careers as certified security professionals. This ensures the right people have the right skills to protect the company, our customers, and our products – now and over time.

2. AVEVA Employees and Cybersecurity ISO

Alongside training and skill development, we provide regular security communication, speaker talks, simulated phishing attempts and global security awareness days to promote a cybersecurity culture and mindset. Employees can also raise any security concerns, suspicions or breaches confidentially using AVEVA's Speak Up policy. This ensures that the problem is raised to the correct individual, and it is resolved. This policy is publicly available and can be found here: Speak Up.

SPEAK UP

"We all have a responsibility to report any concerns about behaviour or decision that could be unethical. If you have concerns, speak up. The sooner you do, the quicker we can take action."

Caspar Herzberg, CEO of AVEVA

3. Security & Data Privacy

AVEVA customers trust us with their critical engineering and operating data throughout the industrial design-build-operate-optimize value chain. We've been on this cybersecurity journey with customer and other stakeholders for decades. Together, we can achieve a strong security posture in alignment with high standard for our industrial ecosystem and national security imperatives.

Our priority remains enabling efficient use of the world's resource via safe and secure services and we are committed to using capabilities which meet or exceed international standards and technology to do so. As both cybersecurity and physical security are interconnected, we take a dual approach to managing our security program.

4. Operating Secure Systems

Our security program follows the requirements of the US National Institute of Standard and Technology (NIST) cybersecurity Framework. We work to continuously improve our cyber defence and response capabilities against an ever-changing threat landscape. As an industrial software company, it is important for us to meet necessary compliance measures, which is shown through our alignment with 800-53, used for security and privacy controls of information and organisations.

5. Secure Development

At AVEVA, we have undergone a range of different audits and certifications to maintain our posture on cybersecurity and to stay ahead of any associated risks and vulnerabilities. In 2024, we achieved ISO 27001 recertification for our R&D organisation and aim to expand this to the rest of the business. We guarantee the operational effectiveness of our data security through internal controls and systems. This is done by annually engaging in a SOC 2 Type II audit by an external independent third-party. Other key certifications we hold includes ISA Secure Security Development Lifecycle Assurance and ISO 9001.

All notifiable data security incidents are reported, and in CY23, there were no reportable incidents. AVEVA also has a business continuity program, which develops and reviews business continuity documentation for critical sites and functions every 12 months.

6. Safeguarding Privacy at AVEVA

New, complex global security challenges emerge on a continuous basis and are a constant part of the software development industry. To combat these challenges, AVEVA must have strong governance mechanisms to protect the security and privacy of the information with which our customers entrust us with. Our Chief Legal Officer has the global responsibility of ensuring data privacy compliance and to report to the Finance and Compliance Committee on a routine basis. This responsibility includes key privacy documentation including our privacy policy, customer privacy policy and cookie policy. During CY23, we did not incur any monetary loss as a result of legal proceeding in relation to user privacy.

AVEVA supplements the security and privacy of our products, IT services and ecosystem with procedural controls. We have set up a number of procedures which employees are required to follow in the event of suspected compromise or breach. These procedures, including rapid escalation, are tested at least annually to ensure they are working correctly and that employees understand how to follow the procedure through.
We occasionally receive information requests from law enforcement authorities in the jurisdictions in which we do business. When this occurs, we respond to lawful requests from such authorities in compliance with applicable legislation.

7. Secure by Design

Our secure by design approach aligns with NIST SP 800-218 Secure Software Development Framework (SSDF) recommended practices for mitigating the risk of software vulnerabilities. The practices span the entire product life cycle from preparing the organization, to design, development and deployment, and response to residual vulnerabilities. Our SSDF implementation uses control requirements in the IEC 62443-4-1 standard which are then certified by ISA Secure.

At AVEVA, we observe high availability and rapid response to security issues that are key factors for industrial software. We especially strive to mitigate any risks related to performance issues, service disruptions and total customer downtime. In CY23, we successfully supported over 2,900 cloud deployments. Our uptime KPI also improves, and we were able to achieve 99.99% uptime across our cloud offerings. Secure development best practices and KPIs as above are measured to drive continuous improvement.

A common set of secure by design principles have been endorsed by global authorities. AVEVA is committed to engagement for progress on the international conversation about key priorities, investments, and decisions necessary to achieve a future where technology is safe, secure, and resilient by design and default. AVEVA is also engaged with critical infrastructure protection initiatives sponsored by the US Cybersecurity Infrastructure Security Agency and the US Department of Energy.

8. Cybersecurity Governance

Cybersecurity governance is part of AVEVA's overarching risk management. AVEVA has established a Security Executive Leadership Council and Security Risk Management Committee.

The Security Executive Leadership Council informs the organisation's executive team on a monthly cadence to set strategic priorities and annual objectives and optimize risk reduction with overall business objectives. It is chaired by AVEVA's General Counsel and has CEO, CFO, CPO, and Chief of Staff as members, with CISO (SVP Digital Security) reporting to the Council. All members of the committee engage and oversee AVEVA's cybersecurity strategy and procedures. The committee ensures that any actions discussed are acted upon, any audit findings have been resolved, and controls have been put in place to prevent the issues from reoccurring.

The Security Risk Management Committee informs the organisation's executive team on a monthly cadence to directly monitor and evaluate operational performance against security risks, and for operational leaders to provide performance updates, and have timely resolution of issues. It is chaired by AVEVA's CISO (SVP Digital Security) and has EVP R&D, CIO, Head of Product Security and representative business function leaders as members. The Security Risk Management Committee makes tactical and operational security risk decisions or escalates to the Security Executive Leadership Council if further guidance and executive support is required.

9. Security Policies

There are number of security policies, which AVEVA employees are familiar with and adhere to. This includes the Cloud Security Policy, Malware Protection, Vulnerability Management, and the Product Lifecycle Policy.
AVEVA's business conduct guidelines also show the work that AVEVA is doing to ensure optimum security of our products and systems. It includes what employees are expected to do and not to do to protect data such as:

- Treating cybersecurity as an integral part of our strategy.
- Building cyber-resilience across the whole digital ecosystem.
- Not sharing the personal data of employees, customers or third parties, except as permitted by AVEVA's data protection policy.

Both the business conduct guidelines and the data protection policy are publicly available and can be found here: Business Conduct Guidelines and Data Protection Policy. Other documents which may be helpful for finding further information on cybersecurity, data protection and privacy at AVEVA can be found on the website.

Learn more by visiting our website at www.AVEVA.com.