Workiva

# Cybersecurity & Data Privacy Statement

# Cybersecurity & Data Privacy Statement

## Cybersecurity

Our Board of Directors remains focused on persistent cybersecurity and data privacy threats through regular reports at every board meeting to the audit committee and a full board report annually.

Our global cybersecurity and data privacy is led by a team with expertise in privacy law, cybersecurity, compliance, risk, audit, and other functions who assist with decisions for escalated issues. The enterprise information security program and team is led by our Chief Information Security Officer (CISO), who works collaboratively across the organization to ensure protection of our customers' data.

Workiva aligns to the following security frameworks and certifications:

- SOC 1 Type 2
- SOC 2 Type 2
- FedRAMP (Moderate)
- HIPAA
- GDPR
- ISO 27001

To maximize security and privacy, Workiva also offers the following:

- Encryption in transmission and at rest
- Advanced permissions and data authorization
- SSO with SAML and two-factor authentication
- SCIM provisioning compatibility
- Bring Your Own Key (BYOK) Management

In addition, the Cybersecurity Working Group includes experts from privacy, legal, compliance, risk, audit, and other functions who assist with decisions for escalated issues. We manage risks related to cybercrime using a variety of controls and capabilities, including but not limited to:

- Identity and access management
- Data protection
- Phishing simulation
- Firewalls
- Encryption

# Cybersecurity & Data Privacy Statement

- Penetration testing
- Software security
- Intrusion prevention, detection and monitoring systems
- Threat intelligence

In 2019, Workiva was authorized as a Moderate Impact Cloud Service Provider under the Federal Risk and Authorization Management Program (FedRAMP). Workiva achieved the Moderate authorization one year after receiving FedRAMP's Low Impact status, signifying Workiva's ongoing commitment to FedRAMP's stringent cybersecurity requirements.

Workiva achieved certification against ISO 27001 in August 2021. Certification is achieved following an independent assessment of Workiva conformity to the ISO standard. ISO recertification occurs every three years, but to maintain certification, a business must go through annual surveillance audits. These ISO certifications affirm our commitment to privacy and security and demonstrate that our controls are operating effectively.

On an ongoing basis we conduct or facilitate a variety of employee education and awareness training, including for people in specific roles, emerging risks and new technology solutions. In 2020, 100% of employees completed cybersecurity training.

Supplier risk reviews are regularly conducted to help ensure access to and the proper handling of confidential, sensitive and proprietary data. We also engage third-party auditors to evaluate our controls against the SOC1 and SOC2 compliance frameworks.

More Information on Workiva's Security practices can be found at https://www.workiva.com/security

## Data Privacy

Workiva is committed to good stewardship of the personal and business information and assets entrusted to us by our customers, employees, business partners, and other individuals.

Our holistic approach combines data privacy, information security, and data governance to foster a culture of data protection via Privacy by Design principles. These principles are continuously updated through policy, education, and investment.

We've built in the data security measures IT teams want: encrypted in transmission and at rest, SSO with SAML and two-factor authentication, SCIM provisioning compatibility, Bring Your Own Key (BYOK) management, and more.

# Cybersecurity & Data Privacy Statement

All employees are required to follow the Workiva established policies and standards regarding the protection and use of personal information. New employees complete and sign a Confidentiality Acknowledgement, which is also required of all employees on a regular basis.

All employees are required to complete privacy training that varies according to job function and their performance on routine evaluations.

We strive to ensure that all personal information under our care is handled lawfully, fairly, transparently, and securely.

- 100% of employees complete General Security Awareness, or Technical Security Awareness training based on their position within the company on an annual basis. New hires are required to complete training within 5 days of hire date
- 100% of employees complete GDPR training on an annual basis
- 100% of new hires are required to complete securities trading training within 5 days of hire date
- U.S. employees are required to complete HIPAA training on an annual basis

At Workiva, our collaborative approach to data protection and governance positions us well to navigate the complex and evolving global data privacy landscape. Our cross-functional team understands these complicated risks and works together to be in compliance with the law and to create a global culture of data protection and cybersecurity, so we can use data responsibly and strategically in our innovative, customer-focused business strategy.

More information on Workiva's data privacy practices can be found at https://www.workiva.com/legal/privacy-policy