# WORKFRONT SECURITY

As the backbone of many organizations' operational system of record and work management solution, Workfront recognizes the sensitivity of data organizations put into Workfront's products. Workfront's security program is built to securely handle the sensitive data organizations hope to put into Workfront's product. Security is a foundational element of Workfront's product design and operations, allowing you to focus on getting work done, done right, on a platform that has a well-founded security program.

## SECURITY PROGRAM

Workfront's security program is built upon industry-recognized standards, including the AICPA's Trust Services Principles (as demonstrated with Workfront's SOC2 Type 2 Report) and ISO 27000 suite of security standards. We continue to improve our security program over time as part of operating in-line with these standards.

### Encryption

Workfront uses industry-recognized encryption to protect data at rest and in transit. Workfront uses AES 256-bit encryption to protect data at rest in backend data stores and TLS 1.2 (or higher) to protect data in transit.

### Service level agreements

Workfront builds resiliency into its products--utilizing some of the powerful out-of-the-box functionalities enabled by the cloud services providers in use by Workfront--to provide robust service level agreements for uptime for customers. Our SLA guarantees 99.9% uptime with fast response times.

### Data Storage and Isolation

Workfront doesn't store customer data on unencrypted portable media like laptop computers, external hard drives, USB drives, or other portable devices. Your data is always stored properly -- encrypted at rest in our backend databases or object stores in our cloud service providers. Data from one customer cannot be accessed by another customer.

### Access Management

Access to production systems and data is restricted to vetted, authorized personnel. Personnel access is established based on roles, using the principle of least privilege and requires multiple factors to authenticate. Access to data is logged and monitored.

### Application Penetration Testing

On an annual basis, Workfront engages skilled penetration testing organizations to perform external penetration testing of Workfront's products. The scope of these exercises includes testing our applications from an external standpoint, as well as an authenticated user standpoint. Our penetration testers follow known industry standards for good application security, including vetting our applications against OWASP's Top 10.

### Vulnerability Disclosure Program

Found a vulnerability that you'd like to report? We sincerely appreciate you taking time to identify and report your findings to us! Workfront takes these seriously, and uses Bugcrowd -- one of the security industry's best vulnerability disclosure and bug bounty programs -- to intake, triage, assess and, rewards based on validity and severity of your finding(s). If you think you have found a vulnerability in Workfront, please use the form below to submit details about your findings. If you need to contact the security team for something else security-related, please reach out to us at psirt@adobe.com.

### Data Location and Redundancy

Workfront's products are hosted both on Amazon Web Services (AWS) and Google Cloud Platform (GCP). These organizations have robust security and privacy programs, and have commitments to encryption, data security, confidentiality and availability that are maintained at standards that meet those established with Workfront.

AWS and GCP environments are built with resiliency and scale in mind, with the ability to distribute documents and servers between various physical locations within an AWS or GCP region. These regions are built to use geographically dispersed physical locations within the same region to allow for effective redundancy and protection against disaster that might impact a single location within a region.

### Partner Plug-ins and Connectors

Workfront has a vast partner network, which offers various solutions for delivering strategic integrations with independent vendor applications. Safeguards for the tools built and implemented by Workfront partners are established and maintained by the partner. Workfront does not include these plug-ins and connectors during control performance or application penetration testing, and encourages organizations to perform their due diligence on these integrations prior to their use. Any additional information related to the security of these partner plug-ins and connectors should be addressed with the Workfront partner.

### Single Sign-On (SSO)

We encourage you to use your identity and access management technology or SAML-based Single Sign-On (SSO) provider to authenticate to Workfront. Workfront provides a centrally managed Single Sign-On (SSO) configuration that integrates Workfront with your existing SSO solution. Using this functionality, Workfront easily plugs into the most popular SSO solutions, including LDAP, Active Directory, and other Federated solutions that support SAML 1.1/2.0. Using your own provider simplifies access control for organizations, and allows organizations to implement their own.

## SECURITY COMPLIANCE

Workfront has both a SOC2 Type 2 attestation and ISO 27001 certification. For further information about these or to get a copy of these artifacts, please reach out to your Workfront Account Executive.

## MODERN SLAVERY STATEMENT

### Organisation Structure

Workfront, Ltd., Workfront Armenia, LLC, and its parent company, Workfront Inc., (collectively "Workfront") operates its business with utmost honesty and integrity. Workfront is headquartered in Lehi, UT U.S.A and has offices in Basingstoke, UK and Yerevan, Armenia.

Workfront remains committed to improving our practices to ensure that modern slavery or human trafficking are not involved in our business or supply chain.

### Our Product & Supply Chain

Workfront is an international leader in cloud-based modern work management software, offering an operational system of record that preserves the context of all tasks, content, and collaboration, in one place, so that it can be analysed, reported, optimised, and automated.

As a SaaS organisation, Workfront utilises a relatively small supply chain in order to conduct business. A majority of our suppliers provide IT hardware, network services, and software.

### Risk Minimisation

A program of risk assessment in our supply chain is in place and operating to evaluate potential areas where there may be a risk of modern slavery and / or human trafficking. Due diligence is conducted for each supplier prior to on-boarding and annually thereafter, now with the consideration of potentially high risk supply chain services or products and the countries they interact with.

Any supplier found to be at risk of modern slavery and / or human trafficking will not be on-boarded. All suppliers under contract will be required to address any issues raised of risk, otherwise Workfront's relationship with the supplier will be terminated.

This statement was approved on May 22, 2019,

Nathan Jennings,
VP, Assistant General Counsel

## CUSTOMER ACCEPTABLE USE POLICY

This Customer Acceptable Use Policy ("AUP") describes actions that are prohibited when Customer uses the SaaS Services. Workfront reserves the right to suspend Customers access to the SaaS Services as a result of any violation of this AUP by Customer or any of its personnel.

Customer agrees not to upload or otherwise transmit to or through the SaaS Services any of the following material or other content ("**content**"):

- content that infringes the intellectual property rights or other rights of third parties, including without limitation trademark rights, copyrights or rights of publicity or privacy;
- content that contains viruses, trojan horses, worms or any other malicious, harmful, or deleterious programs or code;
- content that is libelous or defamatory or otherwise malicious or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation or age;
- content that promotes or enables any illegal activity; or
- personal financial information or medical information of any nature or any other non-public personally identifiable information that could be legally considered private or sensitive, including without limitation social security numbers, driver's license numbers, birth dates, personal bank account numbers, passport or visa numbers, passwords, and credit card numbers.

If Customer uploads any of the foregoing content to the SaaS Services, upon discovery, Customer agrees to remove such content immediately or, at its reasonable discretion, Workfront may purge such data from the SaaS Services.

In addition, Customer will not use, or encourage or allow any other person or entity to use, the SaaS Services in any of the following manners:

- launching or facilitating a denial of service attack on any SaaS Services;
- adversely impacting the availability, reliability or stability of any SaaS Services;
- attempting to bypass or break any security mechanism on any of the SaaS Services or using the SaaS Services in any other manner that poses a security or service risk to Workfront, to any user of the SaaS Services or to any of Workfront's customers;
- testing, scanning, probing or reverse-engineering the SaaS Services in order to find limitations, vulnerabilities or evade filtering capabilities;
- using the SaaS Services in any manner that may subject Workfront or any third party to liability, damages or danger;
- using the SaaS Services to engage in illegal or fraudulent activity;
- interfering with or disrupting networks connected to the SaaS Services or violating the regulations, policies or procedures of such networks;
- manipulating, removing, altering or in any way obscuring pages or other elements of the SaaS Services; or
- creating a Workfront account for the purpose of competitive evaluation or research or otherwise allowing any person or entity that offers or provides services that are competitive with Workfront's products and/or services to use or access any SaaS Services.

Customer must also ensure that its users (1) do not reveal their account passwords to others or allow use of their accounts by others and (2) protect such passwords from unauthorized use or access. Customer is responsible for setting and maintaining password policies and access controls in Customer's environment and must configure its hardware and software in a way that reasonably prevents unauthorized users from accessing its users' accounts.

## VULNERABILITY DISCLOSURE PROGRAM

**ANAB ACCREDITED**

ANAB
ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS
CERTIFICATION BODY

**ISO 27001 CERTIFIED**

ISO 27001 CERTIFIED
A-LIGN