workiflow

Security Posture Overview

Prepared September 2026 · Contact: security@workiflow.com · Live version: workiflow.com/trust-center

Workiflow is a managed technology partner. When clients trust us with their systems and data, that responsibility is non-negotiable. This document summarises our security posture, compliance status, and insurance coverage, and includes the full register of 69 security controls we operate, continuously monitored through Secureframe, our compliance automation platform. It is intended for client security reviews and procurement processes.

01 / COMPLIANCE STATUS

SOC 2 Type II — AUDIT IN PROGRESS

ISO 27001 — AUDIT IN PROGRESS

Our SOC 2 Type II report will be shared with clients and prospects under NDA once the audit is complete. In the interim, contact security@workiflow.com for documentation to support a vendor review.

02 / HOW WE PROTECT YOUR DATA

Access Controls
Role-based access with least-privilege enforcement. Team members only access the systems and data they need for their specific role, nothing more.

Encryption
Data is encrypted in transit (TLS 1.2+) and at rest. We enforce encryption standards across every system and integration we manage.

Continuous Monitoring
Active vulnerability monitoring and threat detection powered by At-Bay Stance, our embedded security platform, keeping our environment under constant watch.

Incident Response
A documented incident response plan with defined roles, escalation paths, and communication protocols. If something happens, we move fast and transparently.

Vendor & Platform Security
We vet every platform and tool in our stack against security, compliance, and data handling standards before it touches client data.

Employee Security Training
Regular security awareness training and phishing simulations for all team members. Human error is the biggest attack vector. We take it seriously.

03 / INSURANCE & LIABILITY

Errors & Omissions Insurance
Comprehensive professional liability coverage protecting against claims arising from errors, omissions, or negligence in the technology services we deliver.

Comprehensive Cyber Liability
Coverage including data breach response, network security liability, regulatory defense, business interruption, ransomware events, and incident recovery costs.

04 / LEGAL & DATA PROTECTION DOCUMENTATION

Trust Center
www.workiflow.com/trust-center
The live hub for everything in this document — always the current version.

Security Controls Register
www.workiflow.com/trust-center/controls
The live, browsable version of the control register in this appendix.

Privacy Policy
www.workiflow.com/trust-center/privacy
How we collect, use, and protect personal information when you use our services.

Terms of Service
www.workiflow.com/trust-center/terms-of-service
The terms and conditions that govern the use of Workiflow's services and platform.

Data Processing Agreement
www.workiflow.com/trust-center/dpa
Our GDPR commitments and data protection terms for clients processing personal data.

Sub-processors
www.workiflow.com/trust-center/sub-processors
The third-party sub-processors we use to deliver services, with purpose and processing location for each.

69 controls, continuously monitored

The complete register of security controls Workiflow operates, grouped by domain. These controls are monitored continuously through Secureframe as part of our SOC 2 Type II and ISO 27001 programs.

/01 Change Management

8 CONTROLS

Baseline Configurations
Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.

Production Data Use is Restricted
Production data is not used in the development and testing environments, unless required for debugging customer issues.

Segregation of Environments
Development, staging, and production environments are segregated.

Configuration and Asset Management Policy
A Configuration and Asset Management Policy governs configurations for new sensitive systems.

Software Change Testing
Software changes are tested prior to being deployed into production.

Secure Development Policy
A Secure Development Policy defines the requirements for secure software and system development and maintenance.

Approval for System Changes
System changes are approved by at least one independent person prior to deployment into production.

Change Management Policy
A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.

/02 Availability

6 CONTROLS

Business Continuity and Disaster Recovery Testing
The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, management makes changes to the plan based on the test results.

Uptime and Availability Monitoring
System tools monitor for uptime and availability based on predetermined criteria.

High Availability Configuration
The system is configured for high availability to support continuous availability, when applicable.

Business Continuity and Disaster Recovery Policy
A Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.

Backup Restoration Testing
Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.

Automated Backup Process
Full backups are performed and retained in accordance with the Business Continuity and Disaster Recovery Policy.

/03 Organizational Management

17 CONTROLS

Acceptable Use Policy
An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.

Performance Reviews
Internal personnel are evaluated via a formal performance review at least annually.

Internal Control Policy
An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.

Cybersecurity Insurance
Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events.

New Hire Screening
Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.

Advisor Meetings on Security
Senior management meets at least annually to review business goals, company initiatives, resource needs, and risk management activities. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, and audit results.

Organizational Chart
Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes it to internal personnel.

Information Security Program Review
Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.

Information Security Policy
An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.

Code of Conduct
A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.

Background Checks
Background checks or their equivalent are performed before or promptly after a new hire's start date, as permitted by local laws.

Internal Control Monitoring
A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.

Performance Review Policy
A Performance Review Policy provides personnel context and transparency into their performance and career development processes.

Disciplinary Action
Personnel who violate information security policies are subject to disciplinary action, and such disciplinary action is clearly documented in one or more policies.

Security Awareness Training
Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.

Personnel Acknowledge Security Policies
Internal personnel review and accept applicable information security policies at least annually.

Roles and Responsibilities
Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.

/04 Confidentiality

4 CONTROLS

Data Classification Policy
A Data Classification Policy details the security and handling protocols for sensitive data.

Disposal of Customer Data
Upon customer request, data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer requirements.

Retention of Customer Data
Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.

Data Retention and Disposal Policy
A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.

/05 Vulnerability Management

3 CONTROLS

Third-Party Penetration Test
A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.

Vulnerability and Patch Management Policy
A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.

Vulnerability Scanning
Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.

/06 Incident Response

4 CONTROLS

Lessons Learned
After any identified security incident has been resolved, management provides a lessons-learned document to the team in order to continually improve security and operations.

Tracking a Security Incident
Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.

Incident Response Plan
An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.

Incident Response Plan Testing
The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, management makes changes to the plan based on the test results.

/07 Risk Assessment

6 CONTROLS

Risk Assessment and Treatment Policy
A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.

Vendor Risk Assessment
New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.

Vendor Risk Management Policy
A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.

Vendor Due Diligence Review
Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.

Risk Assessment
Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.

Risk Register
A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.

/08 Network Security

5 CONTROLS

Logging and Monitoring for Threats
Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.

Automated Alerting for Security Events
Alerting software is used to notify impacted teams of potential security events.

Restricted Port Configurations
Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.

Network Security Policy
A Network Security Policy identifies the requirements for protecting information and systems within and across networks.

Network Traffic Monitoring
Security tools are implemented to provide monitoring of network traffic to the production environment.

/09 Access Security

10 CONTROLS

Access Control and Termination Policy
An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.

User Access Reviews
System owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.

Least Privilege in Use
Users are provisioned access to systems based on the principle of least privilege.

Encryption and Key Management Policy
An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.

Encryption-in-Transit
Service data transmitted over the internet is encrypted in transit.

Complex Passwords
Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.

Access to Product is Restricted
Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.

Administrative Access is Restricted
Administrative access to production infrastructure is restricted based on the principle of least privilege.

Unique Access IDs
Personnel are assigned unique IDs to access sensitive systems, networks, and information.

Removal of Access
Upon termination or when internal personnel no longer require access, system access is removed, as applicable.

/10 Communications

6 CONTROLS

Communication of Security Commitments
Security commitments and expectations are communicated to both internal personnel and external users via the company's website.

Description of Services
Descriptions of the company's services and systems are available to both internal personnel and external users.

Privacy Policy
A Privacy Policy is published for both external users and internal personnel, detailing the company's privacy commitments.

Terms of Service
Terms of Service or the equivalent are published or shared with external users.

Confidential Reporting Channel
A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.

Communication of Critical Information
Critical information is communicated to external parties, as applicable.