MOSSADAMS

PROPRIETARY AND CONFIDENTIAL

nintex

WORKFLOW CLOUD SYSTEM

RELEVANT TO SECURITY (SOC 3)

AICPA SOC aicpa.org/soc4so SOC for Service Organizations™

February 1, 2019 through April 30, 2019

Moss Adams LLP
999 Third Avenue, Suite 2800
Seattle, WA 98104
(206) 302-6500

Table of Contents

I. Independent Service Auditor's Report 1

II. Assertion of Nintex USA, Inc.'s Management 4

III. Nintex USA, Inc.'s Description of the Boundaries of Its Workflow Cloud System 5

A. System Overview 5

1. Services Provided 5
2. Infrastructure 7
3. Software 8
4. People 11
5. Data 12
6. Processes and Procedures 13

B. Principal Service Commitments and System Requirements 15

C. Complementary User Entity Controls 17

I. INDEPENDENT SERVICE AUDITOR'S REPORT

Nintex USA, Inc.
10800 NE 8th St., Suite 400
Bellevue, WA 98004

To the Management of Nintex USA, Inc.:

Scope

We have examined Nintex USA, Inc.'s accompanying assertion in Section II titled "Assertion of Nintex USA, Inc. Management" (assertion) that the controls within Nintex USA, Inc.'s Workflow Cloud System (system) were effective throughout the period February 1, 2019 to April 30, 2019, to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria).*

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Nintex USA, Inc.'s controls are suitably designed and operating effectively, along with related controls at Nintex USA, Inc. We have not evaluated the suitability of design or operating effectiveness of such complementary user entity controls.

Nintex USA, Inc. uses subservice organizations Microsoft Azure for cloud hosting and identity management, Amazon Web Services for cloud hosting, and Auth0 for identity management. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed and operating effectively. The description presents Nintex USA, Inc.'s Workflow Cloud System; its controls relevant to the applicable trust services criteria; and the types of controls that the service organizations expect to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organization(s) have been implemented or whether such controls were suitably designed and operated effectively throughout the period February 1, 2019 to April 30, 2019.

Service Organization's Responsibilities

Nintex USA, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved. Nintex USA, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Nintex USA, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Nintex USA, Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Nintex USA, Inc.'s service commitments and system requirements based the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Nintex USA, Inc.'s Workflow Cloud System were effective throughout the period February 1, 2019 to April 30, 2019, to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

Seattle, Washington
June 24, 2019

II. ASSERTION OF NINTEX USA, INC.'S MANAGEMENT

nintex

We are responsible for designing, implementing, operating, and maintaining effective controls within Nintex USA, Inc.'s Workflow Cloud System (system) throughout the period February 1, 2019 to April 30, 2019 to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Section III entitled "Nintex USA, Inc.'s Description of the Boundaries of Its Workflow Cloud System" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2019 to April 30, 2019, to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*. Nintex USA, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III entitled "Nintex USA, Inc.'s Description of the Boundaries of Its Workflow Cloud System".

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period February 1, 2019 to April 30, 2019, to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. NINTEX USA, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS WORKFLOW CLOUD SYSTEM

A. SYSTEM OVERVIEW

1. SERVICES PROVIDED

Nintex USA, Inc. (Nintex or the Company) is headquartered in Bellevue, Washington, with offices in the United States, the United Kingdom, Malaysia, Australia, and New Zealand. Nintex strives to make people's jobs easier and their work more productive, from day-to-day tasks, to the most sophisticated business-critical processes.

Nintex Workflow Cloud®, the Company's process automation platform, connects with content repositories, systems of record, and people with easy-to-use tools.

AUTOMATION DESIGN

Nintex Workflow Cloud provides a drag-and-drop interface to design and build workflows without code, and a forms designer to create web forms. Customers can connect structured and unstructured content sources, from legacy systems to modern Software-as-a-Service (SaaS) applications, and automate interactions between cloud services, business applications, document generation, tasks, approvals, and content stores.

EXTENSIBLE INTEGRATION

Nintex Workflow Cloud provides integration with business tools and SaaS applications for common process automation use cases using the Nintex Xtensions™ Framework and Connectors. Customers can create custom connections to third-party services, integrating actions and events using Representational State Transfer (REST)ful Application Programming Interfaces (API).

REPORTING AND MANAGEMENT

Nintex Workflow Cloud provides documented records of all workflow activity, audit trails of individual workflows, and usage trends over time using the Nintex process and intelligence capability and analytics tool. The Nintex process and intelligence capability provides statistical roll-up summaries of workflow instances, tasks, and actions, providing insights into how users are interacting with the product.

USER INTERACTION

Nintex Workflow Cloud provides multiple ways for customers to interact with workflow using documents and forms. DocGen® enables customers to generate documents for a variety of business functions such as sales proposals, contracts, or work orders, and output data to different endpoints. With Nintex Forms, customers can create forms to capture and submit data. Users can also interact with workflow processes directly from email, approving or rejecting tasks without leaving the inbox.

LICENSING

A subscription to the Nintex Platform gives clients the capabilities to manage, automate, and optimize manual processes. The Standard edition includes Workflow, Forms, DocGen, Connectors, and Xtensions.

The Enterprise edition includes the capabilities in Standard, plus the Nintex process and intelligence capability. The Software and Infrastructure of Nintex Workflow Cloud is outlined in **Figure 1** below.

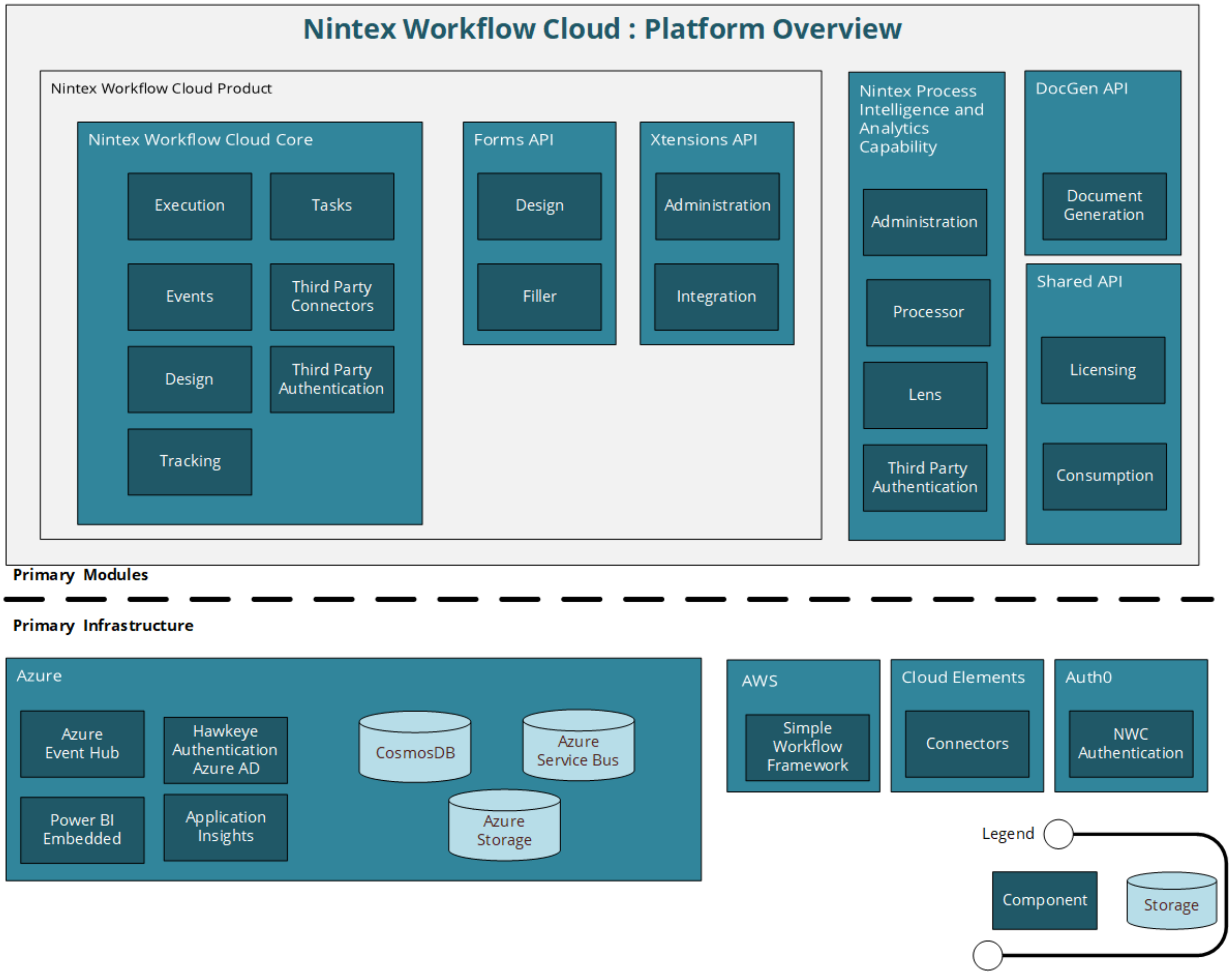

Figure 1. Nintex Workflow Cloud Primary Software and Infrastructure Overview

2. INFRASTRUCTURE

Nintex Workflow Cloud is based on a multi-tenanted, multi-user software-as-a-service (SaaS), hosted in Microsoft Azure (Azure) and Amazon Web Services (AWS). See **Figure 1**.

ACCESS CONTROL

Access to the production environment is restricted to administrator accounts available only to the Production Operations Team. Each person's administrator account is held separately from their primary account for additional security. Development Teams have read-only access to the diagnostic tools of their product in the production environment but cannot access data.

CONTAINER ARCHITECTURE

The Nintex Workflow Cloud Core module (see **Figure 1**) consists of several components and microservices deployed in highly-available container-services and virtual machines in Azure, with specific components hosted in AWS.

PLATFORM-AS-A-SERVICE (PAAS) ARCHITECTURE

The DocGen API, Forms API, Xtensions API, and Shared API modules (see **Figure 1**) are built using .NET and are deployed in highly-available Azure PaaS environments.

DATABASES AND DATA STORAGE

Nintex uses Azure storage technologies to manage customer and application data. All storage technologies provide a minimum standard of Transparent Data Encryption (TDE), with further encryption employed for sensitive data.

All modules except Licensing provide regular data backups on a rolling 90-day schedule for service availability. Backups are geo-replicated to another region at least daily. The Licensing API does not store data; recovery of the Licensing API is via the artifacts on the deployment server which is backed up weekly with 30-day retention.

EXTERNAL SERVICES

MICROSOFT AZURE

Nintex Workflow Cloud makes extensive use of the Azure platform technologies to provide services, including but not limited to:

- ***Storage Technologies:*** Table Storage, Blob Storage, Queue Storage, SQL server, Cosmos DB, Redis, and Data Factory
- ***Computing Technologies:*** Virtual Machines, Container Services, Cloud Services, Functions, and App Services
- ***Networking Technologies:*** Virtual Networks, Load Balancer, Network Security Groups, Traffic Manager, Domain Name Systems (DNS), and Content Delivery Network (CDN)
- ***Integration Technologies:*** Notification Hubs, Event Hubs, Service Bus, API Management, Power BI, and Stream Analytics
- ***Management Technologies:*** Application Insights, Log Analytics, Azure Automation, Identity & Security, Azure Active Directory, Key Vault, and Security Center

AMAZON WEB SERVICES

The Nintex Workflow Cloud Core module uses the Amazon Simple Workflow Service.

INTEGRATION

The Nintex Workflow Cloud Core module (see **Figure 1**) integrates with Cloud Elements for Connectors, a third-party API integration service. Cloud Elements stores user credentials for some third-party SaaS services, and monitors designated third-party events to trigger workflows. All credentials, tokens, and secrets are encrypted with AES256 encryption.

The Nintex Workflow Cloud Core module (see **Figure 1**) integrates with the third-party email provider, SendGrid. This service is used to send emails from within a workflow, such as the Send an Email and Express Approval actions, and to send user-related emails from the product. Nintex Workflow Cloud sends emails using the SendGrid API endpoint over Transport Layer Security (TLS).

AUTHENTICATION

The Nintex Workflow Cloud Core module (see **Figure 1**) integrates with Auth0, a third-party identity management service. Auth0 securely stores the usernames and passwords of Nintex Workflow Cloud users, as well as information such as the tenancies they are permitted to access within an organization, and the role they have within each tenancy.

The Nintex process and intelligence capability Product module (see **Figure 1**) integrates with Azure Active Directory (Azure AD), a third-party identity management service. Azure AD securely stores the usernames and passwords of the Nintex process and intelligence capability users.

APPLICATION MONITORING AND ANALYTICS

Nintex Workflow Cloud uses the following third-party services for monitoring and analytics: Microsoft Azure, which provides infrastructure monitoring; Google Analytics, which collects anonymous usage telemetry; DataDog, which provides application and system monitoring for cloud-based services; and Papertrail, which collates application and system logs for analysis. These services provide usage statistics, system diagnostics, and performance and page level statistics for troubleshooting and improvement. No personal information is collected or stored by these services.

3. SOFTWARE

Nintex Product Teams, incorporating both developers and testers, work together with the Product Management, Quality Assurance, Security, Technical Content, Production Operations, and User Experience and Design Teams to design, develop, and test Nintex Workflow Cloud.

NINTEX WORKFLOW CLOUD

Nintex Workflow Cloud consists of primary modules and infrastructure, integrated with external third-party services. See **Figure 1**.

There are several software safeguards implemented for Nintex Workflow Cloud. Code is reviewed and approved for each submission prior to check-in. Pre-release, static vulnerability scans (via Snyk and Veracode) are performed to test the product for vulnerabilities. The ability to deploy and manage the production environments is restricted to the Production Operations Team. Additionally, an external vendor performs penetration tests every two years.

Nintex also records telemetry on various aspects of the service, anonymized and aggregated derivatives of this data are collected and used for service growth and measurement statistics, and to ensure optimum service delivery.

PRIMARY MODULES

NINTEX WORKFLOW CLOUD CORE

The Nintex Workflow Cloud Core module (see **Figure 1**) enables users to design, publish, and execute workflows. It is responsible for managing integrations with all other modules.

The Nintex Workflow Cloud Core module (see **Figure 1**) uses a container-based architecture built with NodeJS, Ruby, React, and AngularJS in Linux and Windows operating environments. ThoughtWorks GoCD, and Microsoft Azure DevOps are used to automatically deploy infrastructure and applications.

FORMS API

The Forms module (see **Figure 1**) enables users to design public web forms that can be viewed and submitted directly via a public URL or embedded on an external site. The web form design resides in Nintex Workflow Cloud and is retrieved on demand by the Forms API. A submitted form is sent to the Forms API, which uses the Nintex Workflow Cloud API to trigger a workflow or respond to tasks using the form data. Form data is transmitted over TLS. The processing of form data is not TDE-protected. The Forms API does not retain data from the form submission.

The Forms software stack consists of .NET and AngularJS. The software is hosted in Azure using App Services. Microsoft Azure DevOps are used to automatically build and deploy infrastructure and applications.

PROCESS AND INTELLIGENCE CAPABILITY PRODUCT

The Nintex process and intelligence capability Product module (see **Figure 1**) provides analysis and insight into a workflow's performance and efficiency. The Nintex process and intelligence capability securely stores user data in Azure storage and transmits over TLS.

The Nintex process and intelligence capability software stack consists of .NET and AngularJS. The software is hosted in Azure using SQL Server database pools, App Services, and Power BI Embedded Integration. Team City and Microsoft Azure DevOps are used to manually deploy infrastructure and applications.

XTENSIONS API

The Xtensions API module (see **Figure 1**) stores and manages connections between Nintex Workflow Cloud and third-party SaaS systems, including those connected via Nintex Xtensions. The SaaS provider determines the authentication protocol and may use OAuth, API keys, or Basic. All connection credentials are encrypted using AES in Cipher Block Chaining mode, with a 256-bit key, which is stored in a Key Vault. Nintex Workflow Cloud does not store user credentials and makes all requests directly to the SaaS system.

The Xtensions software stack consists of .NET and AngularJS. The software is hosted in Azure, using Azure API Management, Table Storage, Key Vault, and App Services. Team City and Microsoft Azure DevOps are used to manually deploy infrastructure and applications.

DOCGEN API

The DocGen API module (see **Figure 1**) passes data into document templates to generate documents for use in a workflow. Generated documents are only processed in memory (RAM) and are purged after being returned to the workflow.

The DocGen software stack consists of .NET hosted in Azure, using the Azure SQL database, App Service, and Virtual Machines. Bitbucket, Team City, and Octopus Deploy are used to automatically build and deploy infrastructure and applications.

SHARED SERVICES

AUTHENTICATION

The Nintex Workflow Cloud Core module (see **Figure 1**) has an authentication service that provides user identity and access management functionality and additionally integrates with a third-party vendor, Auth0, to provide secure authentication to Nintex Workflow Cloud tenancies.

The authentication service software stack consists of NodeJS and ReactJS. The service is hosted in Azure, using Azure Cosmos DB, Key Vault, Function App, and Table Storage.

The Nintex process and intelligence capability Product module (see **Figure 1**) integrates directly with Azure AD, a third-party identity management service. Azure AD securely stores the user identity and passwords.

SHARED API – LICENSING

The Licensing module (see **Figure 1**) monitors the use of tenancies, including the number of workflows created and billable actions used by a tenancy.

The Licensing software stack consists of .NET and Salesforce APEX. The software is hosted on Azure, using Azure Web Apps, Service Bus, and Microsoft Logic App. Microsoft Azure DevOps is used for local builds and to manually deploy infrastructure and applications.

PRODUCT TEAMS

Nintex software development engineers develop the Nintex production software. Nintex Development Teams use Jira or Microsoft Azure DevOps for development, build management, and work item tracking. Nintex product testing teams perform system and regression testing across development and testing environments.

Development Teams use the Company-approved Secure Software Development Life Cycle (SDLC) Guidelines to identify and manage potential security issues. Software is developed in accordance with the product team code standards, which cover coding styles and conventions.

Product Management follows a framework that aligns with Agile practices, which include phases of ideation, feasibility, validation, construction, and pre-release and post-release measurement to ensure development activities are maintained at a consistent quality and cadence.

4. PEOPLE

The Nintex Board of Directors (BOD) reviews the budget and organization structure during the annual business planning meeting. Management reviews budget, organizational reporting lines, and reporting structure in quarterly business reviews. The reporting structure is revised as necessary to address the Company's risk.

Nintex has a staff of over 500 employees organized in the following functional areas:

Staff	
Senior Management Team	Consisting of the Chief Executive Officer (CEO) and other Executive and senior staff responsible for running various functional units below: • CEO • Chief Financial Officer (CFO) • Chief Technology Officer (CTO) • Chief Legal Officer (CLO) and Information Security Officer (ISO) • Chief Customer Officer (CCO) • Chief Product Officer (CPO) • Chief Marketing and Strategy Officer (CMSO)
Research and Development	Staff responsible for researching and developing key innovations to advance the Nintex platform technologies, including overall product strategy and the development of a product roadmap.
Operations, Practices & Security	Staff responsible for managing operations, security, and quality management.
Customer Success & Support	Staff responsible for providing timely technical support to customers and ensuring customers maintain a positive, productive experience with the Nintex brand.
Marketing	Staff responsible for promoting the Company and communicating a clear, consistent brand across all channels.
Sales	Staff responsible for sales and the development and maintenance of key strategic Nintex partnerships worldwide.
Accounting, Finance, IT, and Human Resources	Staff responsible for managing the fiscal health and day-to-day operations of the Company, including maintenance of corporate resources, and recruitment, training, and retention of staff.

RECRUITING AND TALENT ACQUISITION

Job openings are posted on the Nintex corporate website, as well as on online job sites. Before an offer of employment is made, Nintex conducts interviews and background checks, as allowed by local law, requiring two or more references and employment verification from the successful candidate's previous employer. Interviews are conducted with one or more members of the relevant team.

ORIENTATION AND PERSONNEL MANAGEMENT

As part of the onboarding program, new employees and contractors are required to review and sign to acknowledge the Employee Handbook. Every employee undergoes annual training on the Nintex security policies and procedures, including physical security, data handling, anti-phishing, and web security.

5. DATA

The Nintex Workflow Cloud Product (see **Figure 1**) stores tenancy information, user authorization information, workflow design and metadata, third-party metadata used in workflow triggers. Nintex Workflow Cloud also stores instance state (workflow start variables and the actions performed) for 90 days after the completion of workflows.

The Nintex Workflow Cloud Product (see **Figure 1**) transmits all communication via TLS, using a certificate from a well-known certificate provider. Data is stored using Azure storage technologies, which provides TDE encryption as standard.

The Nintex process and intelligence capability Product module (see **Figure 1**) collects data from Nintex Workflow Cloud Core module (see **Figure 1**) for the workflow metadata when it is published, deleted, or when a workflow instance is run. Task descriptions, the values stored in variables, and the results of actions are not recorded by the Nintex process and intelligence capability.

The Nintex process and intelligence capability transmits all communication via TLS, using a verified certificate from a well-known certificate provider. Date is stored using Azure storage technologies, which provide TDE as a standard.

STORAGE OR PROCESSING OF DATA

Nintex Workflow Cloud uses Azure storage technologies to process and store data, including but not limited to:

- Access and refresh tokens to third-party services
- User credentials to third-party services that require API keys or basic (username and password) authentication
- First and last names of users, their roles within Nintex Workflow Cloud, and tenancy information
- Workflow designs and metadata
- The subject, description, assignee, and response of tasks
- Generated documents
- Files stored in third-party Enterprise File Sync and Share services
- Tenancy information such as the URL domain and licensing
- Metadata received from third-party events that trigger workflows

- Workflow tracking data: actions, tasks, and instance list messages, including the date and time they occurred
- Workflow instance state: workflow and start variables and the actions performed by the workflow, including data (but not files) submitted by forms
- Files uploaded directly to the customer's Enterprise File Sync and Share (EFSS) (See Files below)
- The Nintex process and intelligence capability collects all details regarding when a workflow is published, run, or deleted

FILES OF DATA

When generating a document using the using the DocGen API (see **Figure 1**), Nintex Workflow Cloud temporarily uploads the document template files and any required images from the customer's EFSS system to a multi-tenanted Blob Storage protected by a Microsoft Shared Access Signature (SAS) token. The document template files are automatically removed within one hour of being uploaded to Blob Storage.

DocGen-generated documents are downloaded directly from the Document Generation engine (see **Figure 1**) to the client's EFSS and are not stored by Nintex Workflow Cloud.

To interact with files, Nintex Workflow Cloud uses file variables, which point to the location on the user's EFSS where the file is stored, allowing the workflow to perform actions on the file using the EFSS API rather than having to download or process the file. When an EFSS file's content is required by a workflow action, the file is downloaded, processed in memory (RAM), and purged after use. File content is not stored in the workflow nor in a queue.

6. PROCESSES AND PROCEDURES

Nintex uses security-centric procedures defined in a collection of policy and guideline documents. The Nintex Governance Risk and Compliance (GRC) Team creates and maintains these documents, to help employees clearly understand expectations for operating and working at Nintex, including all its products and services. Nintex requires that all employees complete security training on an annual basis, with much of the training content based on the information contained in these policy and guideline documents and the Company's SOC 2 Controls.

Policies	
Access Management Policy	Outlines security practices to prevent unauthorized access to Nintex and customer information systems. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation in accordance with our business requirements, as well as relevant laws and regulations.
Asset Management Policy	Outlines requirements for the identification and protection of physical hardware connected to information systems at Nintex. The level of protection is dependent on the level of classification, its business use, and any applicable regulatory requirements or contractual obligations for those assets.

Policies	
Information Security Policy	Outlines management direction and support for Information Security Program and Policy activities at Nintex. This policy defines the necessary rules for security protection, and it ensures secure and reliable operations in accordance with our business requirements as well as relevant laws and regulations.
Password Management Policy	Governs password usage of all Nintex employees, contractors, and interns ("users"). It helps protect Nintex, its users, vendors, partners, and customers from legal liability or other harm due to a compromised network or system.
Patch Management Policy	Outlines the processes to ensure that information systems at Nintex, including applications and software, are patched in a timely manner to reduce or prevent the possibility of unwanted intrusion or exploitation from open vulnerabilities.
Security Incident Response Policy	Outlines the requirements for handling a security incident within the Nintex organization. This policy describes appropriate responses to incidents that threaten the confidentiality, integrity, and availability of information assets. Together with the Nintex Security Incident Response Guidelines, this policy establishes an effective incident response program to detect, analyze, prioritize, and handle security incidents.
Vulnerability Management Policy	Outlines scanning processes for scannable endpoint devices. This policy establishes the requirements for scanning, validation of vulnerabilities, and remediation in accordance with the timeframes outlined in the Vulnerability Management and Patch Management Guidelines.

Guidelines	
Account Provision and De-provision Guidelines	Outlines the necessary requirements to create, modify, delete, and maintain user accounts inside the Nintex enterprise environment.
Cryptography Guidelines	Establishes a framework for the proper use of cryptography in Nintex products and services. This guideline informs software development requirements where there may be a choice of implementation functions to use. It covers TLS, symmetric and asymmetric algorithm requirements, and hash function requirements.
Data Handling Guidelines	Establishes a framework for the proper handling of Nintex customer data to ensure data is appropriately handled based on the level of sensitivity, value, and criticality to Nintex.
Enterprise Change Management Guidelines	Provides direction and support for performing production change activities in a consistent manner, including requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change.
Password Guidelines	Provides the framework for how Nintex employees should create, rotate, and protect passwords for Nintex information systems.
Release Management Guidelines	Provides guidance regarding release management for Nintex and supports the Nintex mission to address the needs of its customers and users. These guidelines define requirements for planning, including contingency and rollback planning, releases versus launches, release management checklists, and communications.
Secure SDLC Guidelines	Provides a framework for the SDLC at Nintex. It assists with the identification and mitigation of vulnerabilities.
Security Incident Response Plan	Provides a framework for the Nintex incident response process for security incidents to inform employees on the standard operating procedures during a security incident.
Security Logging and Monitoring Guidelines	Provides information for logging and monitoring activities on Nintex enterprise information systems and guidance on the security controls to consistently fulfill these requirements.

Guidelines	
Vendor Management Guidelines	Provides the procedures for managing Nintex vendor procurement and review lifecycle. This ensures that Nintex obtains the best value for a product or service while controlling exposure to vendor-related risk.
Vulnerability Management Guidelines	Provides a framework for vulnerability management at Nintex, ensuring that Nintex has baseline security across all enterprise information systems where Nintex data may be stored.

SECURITY AND COMPLIANCE

Under the guidance of the Nintex Information Security Practice Team (InfoSec Team), the Development and Production Operations Teams document processes and procedures to support secure development, maintenance, and production of Nintex products and services.

These documents may include:

- Incident response runbooks
- Test plans and test cases
- Operations and productions support procedures
- Logging and monitoring plans

PRODUCT RELEASES

All product releases follow a release plan process, which includes identification and management of security issues, quality-assurance processes, such as static code analysis to maintain code integrity, and contingency or rollback procedures for each release. Changes to the production environment follow a change management procedure, including planning and review, implementation testing, and the development of contingency or rollback procedures.

PRODUCT DOCUMENTATION

Product documentation is hosted in a repository, including a list of tasks and activities that are necessary to the project's success, the owners of those tasks, and timelines for completion. Depending on the nature of the project, additional documentation such as deployment plans, design documents, test plans and test cases, and release notes may also be developed.

B. PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS

Nintex's commitments to its customers are documented and communicated in the Nintex Master Subscription Agreement and the Nintex Privacy and Customer Use Policies. All customers must enter into an agreement with Nintex in order to access the service. The Privacy and Customer Use Policies are accessible to through Nintex's website, and are updated regularly.

The Online Privacy Policy includes the following commitments:

- Nintex does not solicit, does not require and you should not disclose to Nintex any sensitive personal data via our website.
- Customer personal data is processed in accordance with applicable data protection and privacy laws.
- Nintex is responsible under the Principles for the processing of Personal Data it receives under Privacy Shield and subsequently transfers to third parties acting as agents on their behalf.

PRINCIPAL SERVICE REQUIREMENTS

Nintex service system requirements are documented and communicated to employees through internal policies, standards, and procedures. These materials are available to all team members and they agree to comply with these materials at the date of hire. The requirements include:

- System access be implemented according to need-to-know, least privilege, and separation of duties.
- System changes are managed according to change control procedures.
- System components are hardened consistent with internal standards.
- Confidential data is encrypted in transit and at rest.
- System components are monitored for security performance.
- Risks are managed and acknowledged by executive leadership.

C. COMPLEMENTARY USER ENTITY CONTROLS

Nintex USA, Inc.'s Workflow Cloud System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Workflow Cloud System. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Nintex USA, Inc. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

	Complementary User Entity Controls
1	Understanding and complying with their contractual obligations to Nintex.
2	Immediately notifying Nintex of suspected or confirmed information security breaches such as compromised user accounts or passwords.
3	Developing disaster recovery and business continuity plans that address their ability to use or access Nintex Workflow Cloud.
4	Protecting end-points to thwart malicious software from entering the Nintex Workflow Cloud execution environment.
5	Notifying Nintex of changes made to technical or administrative contact information in a timely manner.
6	Designating internal personnel who are authorized to request user additions, deletions, and security level changes.
7	Managing the user access controls for provisioning and deprovisioning user accounts. This includes enforcement of password policies, management of shared accounts, and authorization approvals.
8	Restricting administrative privileges to approved need-to-know personnel.
9	Securely managing the connectors including confidential management of account credentials, disabling connections no longer required, and managing need-to-know access to shared account information.
10	Understanding and defining data storage requirements. Securely configuring any EFSS systems or other systems where files are eventually stored.
11	Managing the confidentiality and integrity of the distribution of authentication tokens used to start component workflows.
12	Managing the need-to-know and least privilege when sharing workflows.