Proprietary & Confidential

Nintex Automation Cloud and Process Manager Systems

SOC 3

Relevant to Security

Integrated SOC 3 Report Prepared in Accordance with the AICPA Attestation Standards and IAASB ISAE No. 3000 (Revised) Standards

MAY 1, 2022 TO APRIL 30, 2023

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report 1

II. Nintex USA, Inc.'s Assertion 4

III. Nintex USA, Inc.'s Description of the Boundaries of Its Nintex Automation Cloud and Process Manager Systems 5

A. System Overview 5

1. Services Provided 5
2. Infrastructure 9
3. Software 12
4. People 16
5. Data 17
6. Processes and Procedures 19

B. Complementary Subservice Organization Controls 21

C. Complementary User Entity Controls 22

D. Principal Service Commitments and System Requirements 23

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 "Nintex USA, Inc.'s Assertion" (assertion) that the controls within Nintex USA, Inc.'s Nintex Automation Cloud and Process Manager Systems (system) were effective throughout the period May 1, 2022 to April 30, 2023, 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*, in AICPA *Trust Services Criteria*.

Nintex USA, Inc. uses the following subservice organizations:

- Microsoft Azure for cloud hosting and identity management
- Amazon Web Services for cloud hosting
- Auth0 for identity management

Nintex USA, Inc.'s description of the boundaries of its system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Nintex USA, Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Nintex USA, Inc.'s description of the boundaries of its system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.'s service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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 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 AICPA and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. 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 on the applicable trust services criteria

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 Nintex Automation Cloud and Process Manager Systems were effective throughout the period May 1, 2022 to April 30, 2023, 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
December 8, 2023

II. Nintex USA, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nintex USA, Inc.’s Nintex Automation Cloud and Process Manager Systems (system) throughout the period May 1, 2022 to April 30, 2023 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 titled “Nintex USA, Inc.’s Description of the Boundaries of Its Nintex Automation Cloud and Process Manager Systems” 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 May 1, 2022 to April 30, 2023, 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 titled “Nintex USA, Inc.’s Description of the Boundaries of Its Nintex Automation Cloud and Process Manager Systems”.

Nintex USA, Inc. uses the following subservice organizations:

- Microsoft Azure for cloud hosting and identity management
- Amazon Web Services for cloud hosting
- Auth0 for identity management

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Nintex USA, Inc.’s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents Nintex USA, Inc.’s complementary user entity controls assumed in the design of Nintex USA, Inc.’s controls.

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 May 1, 2022 to April 30, 2023, 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 Nintex Automation Cloud and Process Manager Systems

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, South Africa, and Israel. Nintex strives to make people’s jobs easier and their work more productive, from day-to-day tasks to sophisticated business-critical processes.

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

Nintex Process Manager (Process Manager), the Company's process management platform, allows companies to document and share process knowledge across their organization through an online tool aimed at non-technical users.

NINTEX AUTOMATION CLOUD

AUTOMATION DESIGN

Nintex Automation 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 Automation Cloud provides a drag-and-drop interface to design and build workflows without code and a forms designer which can create custom connections to third-party services, integrating actions and events using Representational State Transfer (REST)full Application Programming Interfaces (API).

REPORTING AND MANAGEMENT

Nintex Automation Cloud (via Nintex Analytics Services) 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 Automation 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.

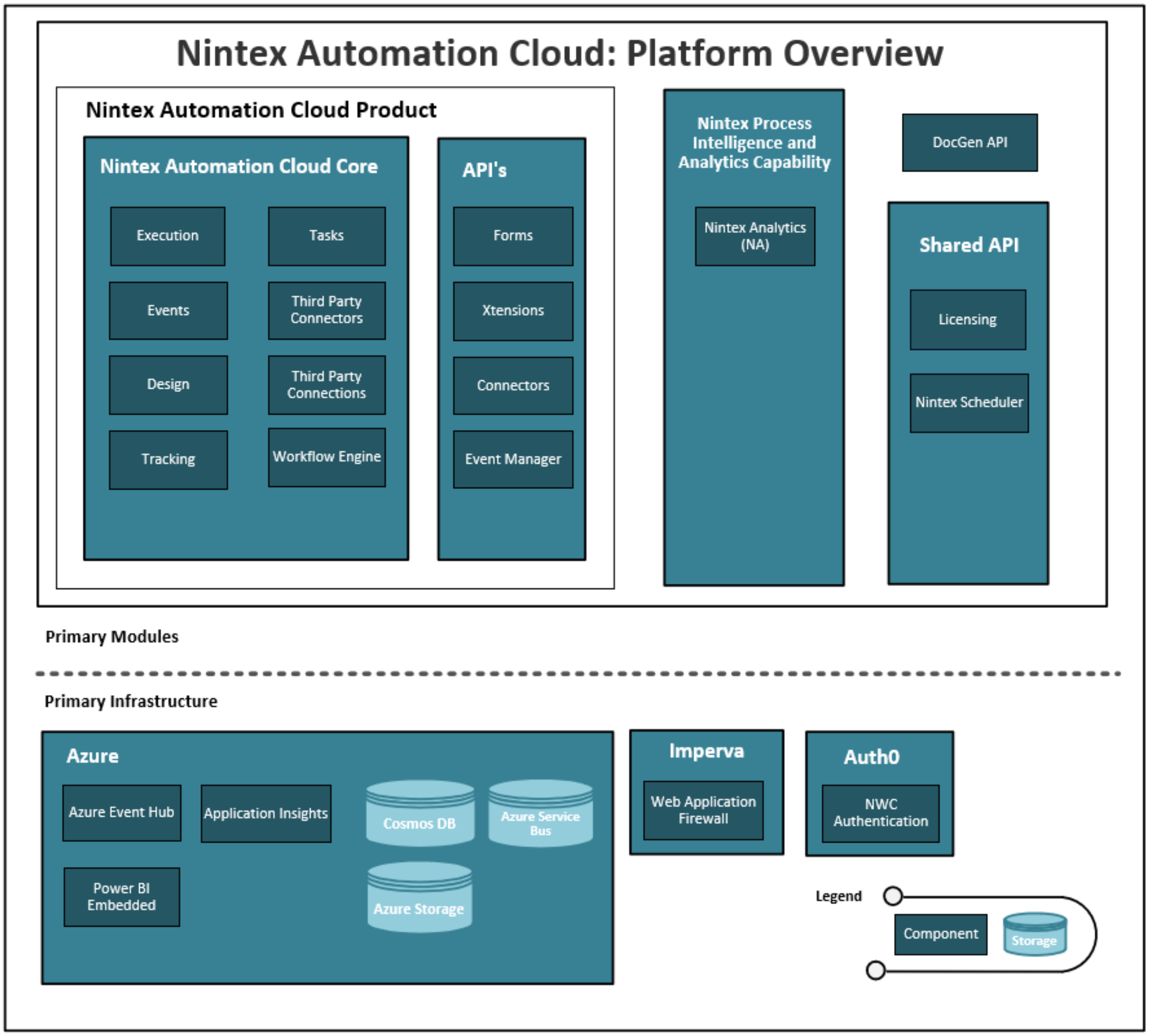

FIGURE 1: NINTEX AUTOMATION CLOUD PRIMARY SOFTWARE AND INFRASTRUCTURE OVERVIEW

NINTEX PROCESS MANAGER

PROCESS MANAGEMENT

Nintex Process Manager is a process management software that enables organizations to build, improve, and share their process knowledge from a central online repository. Nintex Process Manager simplifies process mapping so teams can own and improve their own processes.

Nintex believe that process improvement is a team effort and that everyone across the business should be able to contribute. Nintex Process Manager has been designed with the everyday user in mind. By making processes easy to create, understand, and update, Nintex Process Manager empowers teams to drive process improvements. With clear ownership and accountability, teams can create, use, and update their own process documents and identify and implement opportunities for improvement in their day-to-day work.

RISK AND COMPLIANCE

Nintex Process Manager's risk and compliance add-on provides organizations and teams confidence that their risk management is not just recorded, but operational. Successful risk management depends on ongoing risk awareness across the whole organization. Nintex Process Manager integrates risk and compliance requirements directly into processes, making it an everyday activity, with a live feed updating risk and compliance records automatically.

PROCESS IMPROVEMENTS

Process improvements originate from across an organization and materialize in many forms. The improvement add-on tracks improvement from these multiple sources which could include process suggestions, product defects, quality issues, customer complaints, and non-conformance incidents. The add-on handles logging and tracking improvements integrating completely with processes at every step.

Stand-alone incident and improvement systems risk isolating ideas and events from the core processes that they most relate to. Nintex Process Manager builds them into the everyday business of the organization, managing the full lifecycle and integrating incidents into processes, engaging the line of business at every step. Improvement opportunities are captured and tracked through every phase, translating into real actions and value-adding benefits.

AUTOMATION INTEGRATION

The Workflow Generator is a function within Nintex Process Manager that easily integrates workflows into the process management platform. Instead of letting the technical barriers of automation slow down process improvement, the Workflow Generator facilitates an easy and effective way to create automation within a Nintex workflow in a few clicks instead of lines of code.

CHECKLISTS

The Nintex Process Manager checklist feature ties the activities of a process together by connecting responsible team members at every step. Each process activity within the checklist is related to an individual providing timely notification of their involvement in the process and importantly when completed notifying the next team member, ensuring an appropriate level of responsible and accountability. The checklist feature makes available all the process information at the team members fingertips to ensure easy access and compliance. As team members progress through the checklist, their signoff is recorded in for accurate and timely tracking.

REPORTING

The Reporting Application Programming Interfaces (API) enables organizations to query the data stored in their Nintex Process Manager site. This level of access to data provides the opportunity to build custom queries and the flexibility in generating reports for the organizations specific business needs.

The Reporting API adheres to the OData (Open Data Protocol) standard enabling organizations to leverage the reporting tool of choice.

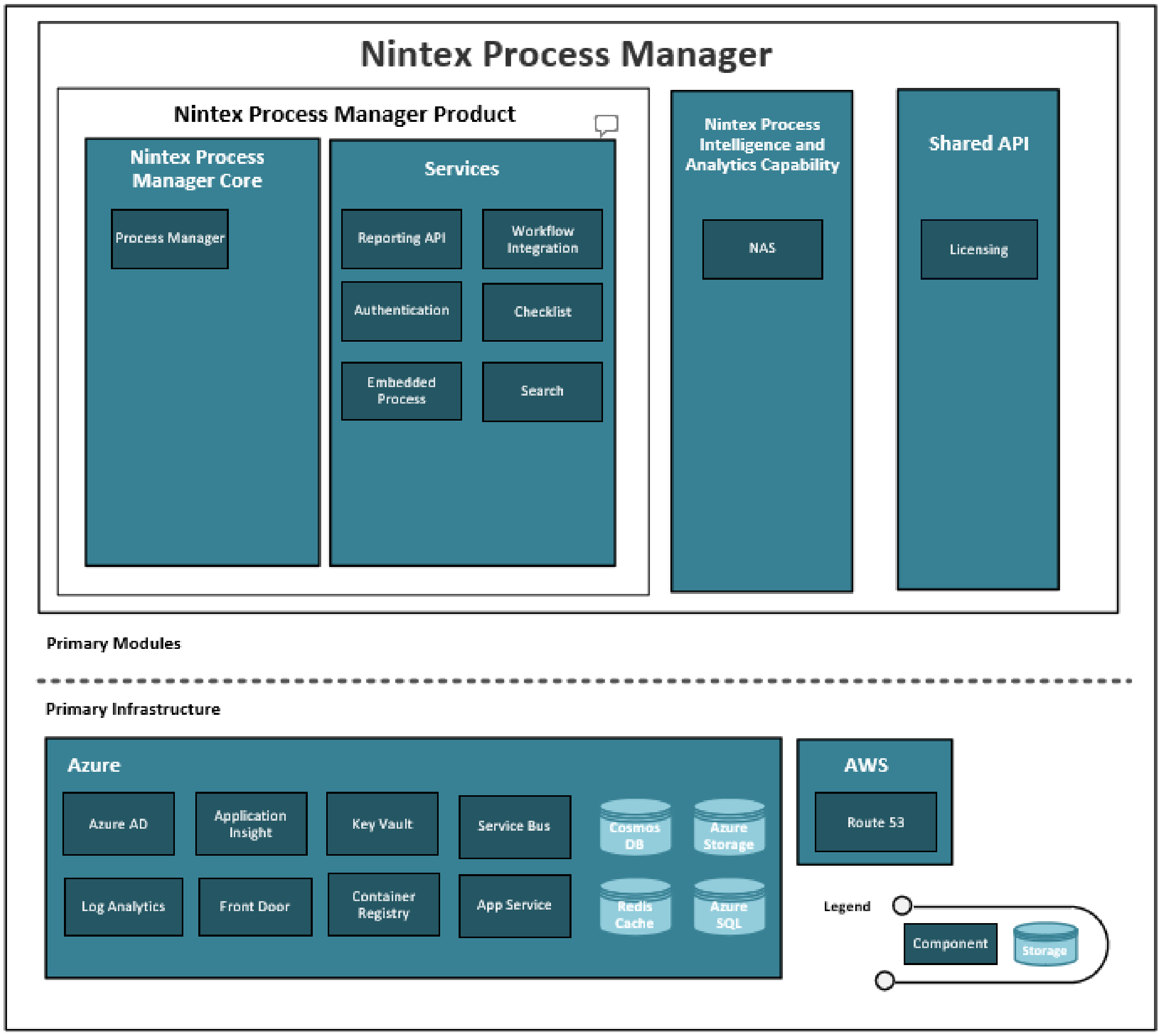

FIGURE 2: NINTEX PROCESS MANAGER SOFTWARE AND INFRASTRUCTURE OVERVIEW

LICENSING

A subscription to the Nintex Platform gives customers 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 Automation Cloud is outlined Figure 1 above.

The Provisioning Service manages creating and licensing of customer tenancies. The Licensing module monitors the use of tenancies.

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.

NINTEX PROCESS MANAGER MOBILE

The Nintex Process Manager mobile app is a read-only app that displays procedural information from Nintex Process Manager web.

The Nintex Process Manager mobile app communicates with Nintex Process Manager via the Nintex Mobile API, using Imperva's application security. Nintex Process Manager and Nintex Mobile API are hosted in Microsoft Azure. All communication is secured via Transport Layer Security (TLS) v1.2, using a verified certificate from a well-known certificate provider. The software and infrastructure of Nintex Process Manager is outlined in Figure 2 above.

2. Infrastructure

Nintex Automation Cloud and Process Manager are based on a multi-tenanted, multi-user software-as-a-service (SaaS), hosted in Microsoft Azure (Azure). See Figure 1 and Figure 2.

ACCESS CONTROL

Privileged access to the production environment is restricted to privileged accounts. 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. Privileged access is enabled just-in-time (JIT) upon approval.

CONTAINER ARCHITECTURE

The Nintex Automation Cloud Core module (see Figure 1) consists of several components and microservices deployed in highly available container-services and virtual machines in Azure.

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 and Infrastructure-as-a-service (IaaS) environments.

Nintex Process Manager runs on PaaS services within the Microsoft Azure data centers in four distinct geographical jurisdictions (Australia, U.S., Europe, Canada, and United Arab Emirates). Each region contains a complete set of services that allow customers to locate both their data and processing within one geographic jurisdiction.

The core of Nintex Process Manager is a monolith (Process Manager Core), which is a full .NET Framework ASP.NET MVC application that runs on Azure Application Service Plans. This is supported with select functionality provided by a number of other microservices that are containerized .NET Core applications that also run on Azure Application Service Plans.

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.

Applicable modules except Licensing provide regular data backups on a rolling 90-day schedule for service availability. Backups are stored 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.

Nintex Process Manager uses Azure PaaS storage technologies to manage customer and application data. The majority of data is stored in Azure SQL databases with a combination of Azure Blob Storage, Azure Cosmos DB, and Azure Redis Cache used for additional storage functionality. All storage technologies are configured to encrypt data at rest. All storage services storing non-temporary data is configured to have regular backups to region redundant storage in a secondary region pair within the same geographic jurisdiction as the primary storage.

NETWORKING

All access to Nintex Process Manager production infrastructure is restricted via Microsoft Azure Virtual Network technology, which restricts access to Azure resources from public Internet Protocol (IP) addresses. Nintex Process Manager web services are made available to the public through a single-entry point to enforce consistent centralized control of routing, firewall, and TLS connections.

EXTERNAL SERVICES

MICROSOFT AZURE

Nintex Automation Cloud and Process Manager make 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. For Process Manager Azure SQL, Blob Storage, Cosmos DB, and Redis Cache are used.
- *Computing Technologies:* Virtual Machines, Container Services, Cloud Services, Functions, and App Services. For Process Manager, the Functions and Logic Apps are used.
- *Networking Technologies:* Virtual Networks, Load Balancer, Network Security Groups, Traffic Manager, Domain Name Systems (DNS), and Content Delivery Network (CDN). For Process Manager, Virtual Networks, Frontdoor, Web Application Firewall, Application Gateway, and Network Security Groups are used.
- *Integration Technologies:* Notification Hubs, Event Hubs, Service Bus, API Management, Power BI, and Stream Analytics. For Process Manager, Service Bus is used.
- *Management Technologies:* Application Insights, Log Analytics, Azure Automation, Identity & Security, Azure Active Directory, Key Vault, and Security Center. For Process Manager, Application Insights, Log Analytics, Identity & Security, Azure Active Directory, Key Vault, and Security Center are used.

AMAZON WEB SERVICES

Nintex Process Manager utilizes AWS Route53 for Domain Name System (DNS) resolution.

INTEGRATION

The Nintex Automation Cloud Core module and Process Manager integrate 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 Automation Cloud sends emails using the SendGrid API endpoint over Transport Layer Security (TLS).

Videos uploaded to Nintex Process Manager are encoded for web distribution using the Brightcove Zencoder service. Videos are sent to Zencoder for encoding and then the resulting encoded video is stored within Nintex Process Manager's Azure Blob Storage. Zencoder does not store the video content.

Nintex Process Manager integrates with the Nintex Automation Cloud to link processes with workflows. Information about the workflows is synchronized with Nintex Process Manager so process users have visibility of which aspects of their processes are automated.

AUTHENTICATION

The Nintex Automation Cloud Core module (see Figure 1) integrates with Auth0, a third-party identity management service. Auth0 securely stores the usernames and passwords of Nintex Automation Cloud users, as well as identity federation details for customers using their own Identity Provider to authenticate with Nintex Automation Cloud.

The Nintex Process Manager users authenticate directly with their Nintex Process Manager tenant, which securely stores the usernames and passwords, as well as information regarding their permissions to difference functionality and resources within their tenancy.

Administrators can choose to connect a Nintex Process Manager tenancy with a Security Assertion Markup Language (SAML)-compliant Identity Provider to allow management of users to be handled outside of the Nintex Process Manager tenancy if desired and provide users with Single Sign-On to their tenancy.

APPLICATION MONITORING AND ANALYTICS

Nintex Automation 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.

Nintex Process Manager uses the following third-party services for monitoring and analytics: Microsoft Azure, which provides infrastructure monitoring, and Datadog, which provides application and system monitoring for cloud-based services. These services provide usage statistics, system diagnostics, performance, and request level statistics for troubleshooting and improvement.

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 Automation Cloud and Process Manager.

NINTEX AUTOMATION CLOUD

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

There are several software safeguards implemented for Nintex Automation Cloud. Code is reviewed and approved for each submission prior to merge. 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 privileged users. Additionally, an external vendor performs penetration testing every year.

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.

PROCESS MANAGER

Nintex Process Manager consists of a monolith, microservices, and infrastructure, integrated with external third-party services.

There are several software safeguards implemented for Nintex Process Manager. Branch protection rules are in place to enforce that all automation tests pass, and all code is reviewed by at least one other approved merger prior to incorporation into the main branch. Infrastructure changes are described as code and adhere to the same review and deployment processes as the application code. Pre-release, static code vulnerability scans (via Veracode) are performed to test the product for vulnerabilities. The ability to deploy to the production environment requires pre-release checks to pass and approval by a nominated approver. Additionally, an external vendor performs penetration testing every year.

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

PRIMARY MODULES

NINTEX AUTOMATION CLOUD CORE

The Nintex Automation 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 Automation Cloud Core module (see Figure 1) uses a container-based architecture built with NodeJS, Ruby, and React in Linux and Windows operating environments. Microsoft Azure DevOps is 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 forms can be designed to be authenticated or public. The web form design resides in Nintex Automation Cloud and is retrieved on demand by the Forms API. A submitted form is sent to the Forms API, which uses the Nintex Automation Cloud API to trigger a workflow or respond to tasks using the form data. Form data is transmitted over TLS.

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, Databricks, and AngularJS. The software is hosted in Microsoft Azure. 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 Automation 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 Automation 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. Microsoft Azure DevOps is 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 subsequently 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.

The generated document is stored temporarily on an encrypted Blob storage while the document is being transferred to its destination. The temporary document is purged subsequently after being returned to the workflow.

NINTEX EVENT MANAGER

Nintex Event Manager (see Figure 1) is a backend service that manages subscriptions to third-party services so that notifications can be evaluated and forwarded to Nintex Automation Cloud. This enables the functionality that is required to start a workflow in response to an action within a third-party service.

The Nintex Event Manager software stack is coded in .NET, hosted in Microsoft Azure, and leverages Azure storage. Microsoft Azure DevOps is used to build and deploy this service.

NINTEX CONNECTORS

Nintex Connectors (see Figure 1) are integration points that run operations in third-party services. They provide backend support for workflow actions that are used in Nintex Automation Cloud.

The Nintex Connectors stack is developed using .NET and hosted in Microsoft Azure. Microsoft Azure DevOps is used to build and deploy this service. Nintex Connectors do not store data.

SHARED SERVICES

AUTHENTICATION

The Nintex Automation 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 Automation 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 Auth0, a third-party identity management service. Auth0 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.

SHARED API – NINTEX SCHEDULER

Nintex Scheduler (see Figure 1) is a backend service that manages the execution of jobs that are configured to run on a specific schedule. It provides functionality such as configuring a workflow to run on a time-based schedule.

The Nintex Scheduler software stack is coded in .NET, hosted in Microsoft Azure, and leverages Microsoft Azure storage. Microsoft Azure DevOps is used to build and deploy this service.

PROCESS MANAGER CORE

The majority of Nintex Process Manager's functionality exists in a monolithic application that is responsible for the core functions of the offering. This includes authentication and authorization, process viewing and editing, improvements, risk and compliance, and tenant-wide configuration.

Process Manager Core module is an ASP.NET Model-View-Controller (MVC) application hosted on Azure Application Service Plans built with .NET Framework, and a mixture of React and JQuery for front-end logic. Microsoft Azure DevOps is used to manage deploy infrastructure and the application.

MICROSERVICES

Several microservices extend the functionality provided by the Process Manager Core monolith including the services below.

SEARCH

Process and document information is sent to the Azure Cognitive Search service for indexing. Users who perform a search within Nintex Process Manager query the Search microservice, which retrieves the results from the Azure Cognitive Search service.

CHECKLIST

Nintex Process Manager allows users to create a checklist based on an existing process, which is then used to track the completion of the tasks within that process. Information about the checklists and which tasks have been completed is stored within the microservice.

WORKFLOW INTEGRATION

Nintex Process Manager integrates with Nintex Automation Cloud through a microservice that captures the linkage between processes within Process Manager Core and workflows within Nintex Automation Cloud. A user needs to authenticate against Nintex Automation Cloud in order to link Nintex Process Manager to Nintex Automation Cloud.

REPORTING

Nintex Process Manager pushes data to Nintex Analytic Services to make it available for reporting. Customer can connect an OData compliant tool (Excel, PowerBI, etc.) to the reporting service to extract their data.

PRODUCT TEAMS

Nintex software development engineers develop the Nintex production software. Nintex Development Teams use 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 950 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) • General Counsel • Chief Customer Officer (CCO) • Chief Product Officer (CPO) • Chief Marketing Officer (CMO) • Chief of Staff • Chief People Officer • Global Head of Sales • SVP, Strategy and Operations • SVP, Channel and Partner
Research and Development	Staff responsible for researching and developing key innovations to advance the Nintex platform technologies, including overall product strategy, Operations, and the development of a product roadmap.
Security and Compliance	Staff responsible for managing information security 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, 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 Automation Cloud Product (see Figure 1) stores tenancy information, user authorization information, workflow design and metadata, third-party metadata used in workflow triggers.

The Nintex Automation 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 Automation 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. Data is stored using Azure storage technologies, which provide TDE as a standard.

Nintex Process Manager (see Figure 2) stores tenancy information, user authorization information, process, risk, improvement and document data, and metadata in a variety of underlying Azure storage technologies, which are configured to encrypt the data at rest.

Nintex Process Manager and services (see Figure 2) transmit all communication via TLS, using a certificate from a well-known certificate provider.

Nintex Process Manager pushes data to the Nintex Analytic Service (see Figure 2), which transforms this data into a structure that allows customers to connect their own reporting tools for advanced reporting.

STORAGE OR PROCESSING OF DATA

Nintex Automation Cloud and Process Manager use 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 Automation Cloud, and tenancy information
- Workflow and Forms designs and metadata
- Data submitted via Nintex Forms as start event data
- The subject, description, assignee, and response of tasks
- Generated documents

- 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 submitted by forms
- Files uploaded directly via a Start Form or Task Form
- The Nintex process and intelligence capability collects all details regarding when a workflow is published, run, or deleted
- First and last names, email address of users, their roles within Nintex Process Manager, and tenancy information
- Process definitions and metadata
- Workflow integration data including Workflow name, Workflow link, Workflow description, Start Event detail
- Files and videos uploaded, and links to files in third-party file systems
- Risk and risk control data and metadata
- Improvement data and metadata
- Tenancy information such as the URL domain and licensing

FILES OF DATA

When generating a document using the DocGen API (see Figure 1), Nintex Automation 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 or temporarily stored by Nintex Automation Cloud.

To interact with files, Nintex Automation Cloud uses file variables, which point to the location on the user's EFSS or Azure Blob Store where the file is stored, allowing the workflow to perform actions on the file without having to download or process the file. When a file's content is required by a workflow action, the file is downloaded, processed in memory, and purged after use.

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.
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.
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. Complementary Subservice Organization Controls

Nintex USA, Inc.'s controls related to the Nintex Automation Cloud and Process Manager Systems cover only a portion of overall internal control for each user entity of Nintex USA, Inc. It is not feasible for the criteria related to the Nintex Automation Cloud and Process Manager Systems to be achieved solely by Nintex USA, Inc. Therefore, each user entity's internal controls must be evaluated in conjunction with Nintex USA, Inc.'s controls, taking into account the types of controls expected to be implemented by the subservice organizations as described below.

Complementary Subservice Organization Controls		Subservice Organization
1	Subservice organizations are responsible for ensuring that processes are in place to identify risks relevant to the subservice organization's infrastructure and supporting systems, evaluate risk and communicate them to management, and perform timely remediation activities.	• Microsoft Azure • Amazon Web Services • Auth0
2	Subservice organizations are responsible for controlling access, logging and monitoring of the systems and underlying infrastructure.	• Microsoft Azure • Amazon Web Services • Auth0
3	Subservice organizations are responsible for establishing, maintaining and disseminating security and usage policies relevant to all systems and underlying infrastructure.	• Microsoft Azure Amazon • Web Services • Auth0

Complementary Subservice Organization Controls		Subservice Organization
4	Subservice organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and customers is added only for authorized individuals, removed when no longer required and reviewed on a periodic basis for the data center where the subservice organization hardware resides.	● Microsoft Azure ● Amazon Web Services ● Auth0
5	Subservice organizations are responsible for implementing processes to ensure that hardware for all systems and underlying infrastructure is disposed in a secure fashion.	● Microsoft Azure ● Amazon Web Services ● Auth0
6	Subservice organizations are responsible for implementing a detailed incident response plan for all systems and underlying infrastructure.	● Microsoft Azure ● Amazon Web Services ● Auth0
7	Subservice organizations are responsible for ensuring that change management process is developed to ensure that changes for all systems and underlying infrastructure are authorized, developed, documented, tested, approved, and implemented in accordance with the policies.	● Microsoft Azure ● Amazon Web Services ● Auth0
8	Subservice organizations are responsible for ensuring that business recovery and continuity procedures are in place and tested regularly for all systems and underlying infrastructure.	● Microsoft Azure ● Amazon Web Services ● Auth0
9	Subservice organizations are responsible for ensuring that a detailed vendor management program exists to assess and manage risks associated with vendors and business partners.	● Microsoft Azure ● Amazon Web Services ● Auth0

C. Complementary User Entity Controls

Nintex USA, Inc.'s Nintex Automation Cloud and Process Manager Systems was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Nintex Automation Cloud and Process Manager Systems. In these situations, the application of specific controls at these user entities is necessary to achieve certain criteria.

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

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place. User entities are responsible for:

Complementary User Entity Controls	
1	Managing the user access controls for provisioning and deprovisioning user accounts. This includes enforcement of password policies, management of shared accounts, and authorization approvals.
2	Restricting administrative privileges to approved need-to-know personnel.
3	Designating internal personnel who are authorized to request user additions, deletions, and security level changes.

Complementary User Entity Controls	
4	Securely configuring any EFSS systems or other systems where files are eventually stored.
5	Managing the confidentiality and integrity of the distribution of authentication tokens used to start component workflows.
6	Managing the need-to-know and least privilege when sharing workflows.
7	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.

D. 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 services (Nintex Automation Cloud and Nintex Process Manager). The Nintex Master Subscription Agreement and Privacy and Customer Use Policies are accessible through Nintex's website and are updated regularly.

The Online Privacy Policy includes the following commitments:

- Nintex does not solicit, does not require, and directs customers not to disclose to Nintex any sensitive personal data via the 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 is 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.

MOSSADAMS