Proprietary & Confidential

System Description of the DocGen for Salesforce System

SOC 3
Relevant to Security

MAY 1, 2021 TO APRIL 30, 2022

MOSSADAMS

Table of Contents

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 DocGen for Salesforce System (system) were effective throughout the period May 1, 2021 to April 30, 2022, 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. uses Microsoft Azure for cloud hosting and identity management and Salesforce for customer identity management (subservice organizations). 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 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.

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. 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 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 DocGen for Salesforce System were effective throughout the period May 1, 2021 to April 30, 2022, 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
October 5, 2022

II. Nintex USA, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nintex USA, Inc.’s DocGen for Salesforce System (system) throughout the period May 1, 2021 to April 30, 2022 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 DocGen for Salesforce 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 May 1, 2021 to April 30, 2022, 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 DocGen for Salesforce System”.

Nintex USA, Inc. uses Microsoft Azure for cloud hosting and identity management and Salesforce for customer identity management (subservice organizations). 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, 2021 to April 30, 2022, 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 DocGen for Salesforce 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, South Africa, and New Zealand. Nintex strives to make people's jobs easier and their work more productive, from day-to-day tasks to sophisticated business-critical processes.

Nintex DocGen for Salesforce, the Company's document generation product offering within the Salesforce platform, allows companies to automate the generation of all their business documents that need to support dynamic data filling. The customer experience is provided directly and seamlessly within Salesforce.

DYNAMIC DOCUMENT GENERATION

Nintex DocGen for Salesforce enables customers, regardless of technical prowess or availability of IT assistance, to automate the creation of sales documents. Quotes, proposals, non-disclosure agreements (NDAs), order forms, contracts, invoices, or any document that drives the business can be deployed using the same documents they have been using for years.

EXTENSIBLE INTEGRATION

Nintex DocGen for Salesforce provides a drag-and-drop interface to design and build document packages without code. This includes the ability to specify which data to use and determine which documents will form the final document(s). Finally, DocGen for Salesforce offers a series of integrated delivery options that determine where the final document will go: back to Salesforce, via Salesforce email, to an e-sign provider, or to a third-party electronic file system.

MANAGEMENT AND REPORTING

Nintex DocGen for Salesforce's package management is installed within an existing Salesforce organization. The package designer experience has the same look and feel as other Salesforce functionality. Customers can leverage all the reporting and customization offered by Salesforce to provide insights into how users are interacting with the product.

USER INTERACTION

Nintex DocGen for Salesforce provides multiple ways for customers' end users to create a document package. Users never leave Salesforce and can either run from a button or lightning component. Customers can also leverage Salesforce automation to call our service via outbound message, process builder, or Apex, a proprietary Salesforce language for server-side scripting.

LICENSING

A standard subscription to the DocGen for Salesforce application gives customers the capabilities to create, deploy, and manage document generation.

The Enterprise edition includes the capabilities in Standard plus the Nintex process and intelligence capability. The software and infrastructure of DocGen for Salesforce is outlined in Figure 1 below.

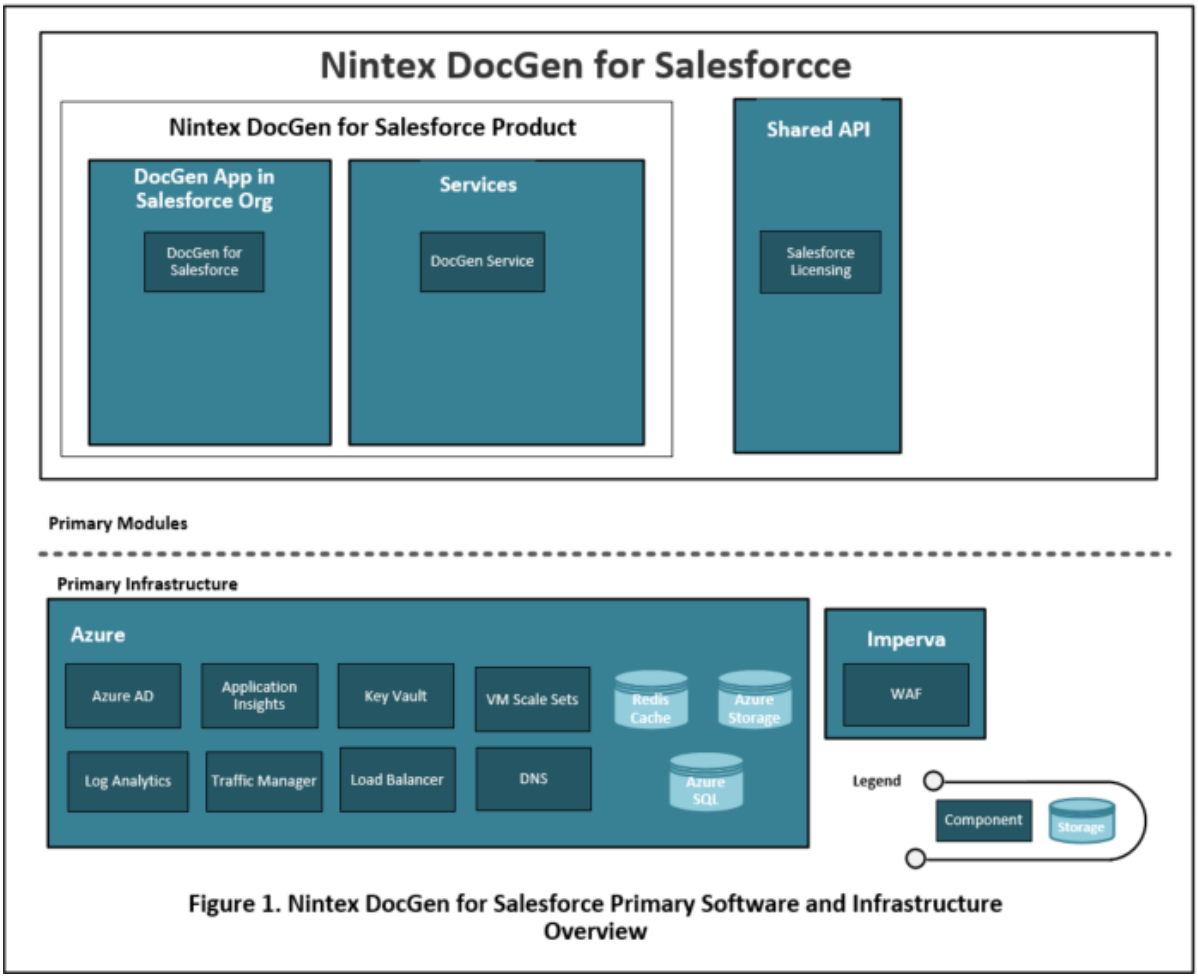

Figure 1. Nintex DocGen for Salesforce Primary Software and Infrastructure Overview

FIGURE 1. NINTEX DOCGEN FOR SALESFORCE PRIMARY SOFTWARE AND INFRASTRUCTURE OVERVIEW

2. Infrastructure

Nintex DocGen for Salesforce is a software-as-a-service (SaaS) application, comprised of a package hosted on the Salesforce AppExchange (Package) and a supporting Document Processing API (API) hosted in Microsoft Azure (Azure). See Figure 1.

ACCESS CONTROL

Access to the production environment is restricted to privileged accounts used solely for the purpose of monitoring and maintaining the production environment. Each person's privileged account is held separately from their primary account for additional security. Development Teams are limited to read-only access to the diagnostic tools of their product in the production environment.

ARCHITECTURE

The Package is installed by customers and hosted on Salesforce infrastructure via Salesforce's own proprietary storage and execution mechanism. The API is hosted in Azure. Virtual Machine Scale Sets (VMSS) are utilized in some areas to provide the ability to scale statically or dynamically. An Automation Account is utilized to apply patches uniformly across VMSS instances and allow for non-production testing prior to patching production VMSS instances. All other components within the API utilize Platform-as-a-Service (PaaS) Azure service offerings to best utilize Azure's scale and availability models.

DATABASES AND DATA STORAGE

Nintex DocGen for Salesforce 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.

AZURE SERVICES

MICROSOFT AZURE

DocGen for Salesforce makes extensive use of the Azure platform technologies to provide services, including but not limited to:

- *Storage Technologies:* File Storage, Blob Storage, Azure SQL, and Redis
- *Computing Technologies:* Virtual Machines, Functions, and App Services
- *Networking Technologies:* Virtual Networks, Load Balancers, Network Security Groups, Traffic Managers, and Domain Name Systems (DNS)
- *Management Technologies:* Application Insights, Log Analytics, Azure Automation, Identity & Security, Azure Active Directory, and Key Vault

INTEGRATION

DocGen for Salesforce integrates with some third-party services to support delivery options for customers. These integrations include API integrations with various e-Signature and storage services. Additionally, DocGen for Salesforce also supports integrations with third-party SFTP, FTPS, and SMTP servers. After completion of a document generation run, the output files and some other metadata, as configured by a customer administrator within the Package, may be sent to those services. All of these integrations are directly controlled by a customer opting into usage and configuring the integration. Integrations use end-to-end encryption for all communication.

AUTHENTICATION

DocGen for Salesforce leverages Salesforce authentication for all customer requests. Before using the Package, customers authenticate with Salesforce directly via standard Salesforce login mechanisms. All requests initiated to the API require a Salesforce access token, allowing the API to verify the authenticity and identity of the customer by leveraging Salesforce's APIs for identity management and authentication.

APPLICATION MONITORING AND ANALYTICS

DocGen for Salesforce uses the following third-party services for monitoring and analytics: Microsoft Azure, which provides infrastructure monitoring; Pendo, which collects anonymous usage telemetry; and Datadog, which provides application and system monitoring for cloud-based services. 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 DocGen for Salesforce.

DOCGEN FOR SALESFORCE

DocGen for Salesforce consists of software within the Package and the API.

There are several software safeguards implemented for DocGen for Salesforce. Code is reviewed and approved for each submission prior to merge. Per release, static vulnerability scans (via Checkmarx and Veracode) are performed to test the product for vulnerabilities. Deployments are performed via automated Continuous Integration/Continuous Delivery pipelines. The ability to initiate deployments and manage the production environments is restricted to team members operating in a Production Operations capacity and via separate, designated, privileged accounts. Additionally, an external vendor performs penetration tests 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.

SALESFORCE PACKAGE

The Salesforce Package enables customer administrators to design and publish DocGen for Salesforce packages (document templates and metadata), manage third-party integrations, and control user permissions to DocGen for Salesforce functionality. The Salesforce Package also enables customer end users to run DocGen for Salesforce packages to generate rich content customized with relevant customer data from Salesforce.

The Salesforce package utilizes Apex and JavaScript to support a rich user experience consistent with Salesforce's design standards. The software is hosted on and served from Salesforce servers and Apex code is executed as part of Salesforce's proprietary processing engine.

DOCGEN FOR SALESFORCE API

The DocGen for Salesforce API supports document processing within the Salesforce Package. When a user initiates a run, a request payload with relevant metadata is sent to the API for processing. The API then performs all work necessary to authenticate the request, fetch the documents and data in question via Salesforce and other service APIs, process and fill the documents, and deliver the resulting files all as defined by the customer administrator's selections within the Salesforce Package. All requests to the API are transmitted over Transport Layer Security (TLS). Customer data is not persisted within the API.

The API software stack consists of .NET and MS SQL via Azure SQL. The software is hosted in Azure using Virtual Machine Scale Sets.

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 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) • Chief Legal Officer (CLO) and Information Security Officer (ISO) • Chief Customer Officer (CCO) • Chief Product Officer (CPO) • Chief Marketing and Strategy Officer (CMSO) • Chief of Staff • Chief Revenue Officer (CRO)
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.

Staff	
Marketing	Staff responsible for promoting the Company and communicating a clear, consistent brand across all channels.
Sales	Staff responsible for sales, sales operations 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 DocGen for Salesforce Product (see Figure 1) stores tenancy information, DocGen package metadata, and configured third-party integration user authorization information. DocGen for Salesforce also stores telemetry related to DocGen runs and error information related to failures.

The DocGen for Salesforce 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.

STORAGE OR PROCESSING OF DATA

DocGen for Salesforce 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 DocGen for Salesforce, and a linkage to their Salesforce tenancy
- DocGen packages
- Generated documents

- Template (input) Files stored in Salesforce or another storage service, as configured by a customer.
- Tenancy information such as the Salesforce domain URL and licensing
- Metadata received from third-party events that trigger DocGen runs
- DocGen run tracking data: including number of and types of files processed, time taken, and the date and time of execution
- Automated DocGen run state: initialization metadata and current progress, including data (but not files) submitted by forms

FILES CONTAINING DATA

When the DocGen for Salesforce API executes a run, (see Figure 1), it temporarily fetches the document templates, specified data, and any required images from the customer's Salesforce organization as defined by the customer Package Administrator in their DocGen package configuration, and processes them, generating one or more output documents. The output documents are then delivered via the customer configured and selected mechanism. The files associated with the run are automatically removed on a schedule after processing. This schedule operates every 30 minutes, removing files older than 1.2 hours (0.05 days).

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.

Policies	
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.

Guidelines	
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. 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 (Nintex DocGen for Salesforce®). The 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.

C. Complementary Subservice Organization Controls

Nintex USA, Inc.'s controls related to the DocGen for Salesforce System 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 DocGen for Salesforce System 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 organization 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 • Salesforce
2	Subservice organizations are responsible for controlling access, logging and monitoring of the systems and underlying infrastructure.	➤ • Microsoft Azure • Salesforce
3	Subservice organizations are responsible for establishing, maintaining and disseminating security and usage policies relevant to all systems and underlying infrastructure.	➤ • Microsoft Azure • Salesforce
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 • Salesforce
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 • Salesforce
6	Subservice organizations are responsible for implementing a detailed incident response plan for all systems and underlying infrastructure.	➤ • Microsoft Azure • Salesforce
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 • Salesforce
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 • Salesforce
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 • Salesforce

D. Complementary User Entity Controls

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

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

MOSSADAMS