Proprietary & Confidential

System Description of the Promapp System

SOC 3
Relevant to Security

FEBRUARY 1, 2021 TO APRIL 30, 2021

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

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 Promapp System (system) were effective throughout the period February 1, 2021 to April 30, 2021, 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 subservice organizations Microsoft Azure for cloud hosting and identity management and Amazon Web Services for Domain Name System web services. Our examination did not include the services provided by 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. 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.

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 Promapp System were effective throughout the period February 1, 2021 to April 30, 2021, 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
August 18, 2021

II. Nintex USA, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nintex USA, Inc.'s Promapp System (system) throughout the period February 1, 2021 to April 30, 2021 to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Section III entitled "Nintex USA, Inc.'s Description of the Boundaries of Its Promapp System" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2021 to April 30, 2021, to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*. Nintex USA, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III entitled "Nintex USA, Inc.'s Description of the Boundaries of Its Promapp System".

Nintex USA, Inc. uses subservice organizations Microsoft Azure for cloud hosting and identity management and Amazon Web Services for Domain Name System web services. 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 February 1, 2021 to April 30, 2021, 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 Promapp 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 Promapp®, 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.

PROCESS MANAGEMENT

Nintex Promapp is a process management software that enables organizations to build, improve, and share their process knowledge from a central online repository. Nintex Promapp 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 Promapp has been designed with the everyday user in mind. By making processes easy to create, understand, and update, Nintex Promapp 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 Promapp'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 Promapp 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 Promapp 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 Promapp 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 Promapp 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 Promapp 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.

LICENSING

The Provisioning Service manages creating and licensing of customer tenancies. The Licensing module (see Figure 1) 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.

The software and infrastructure of Nintex Promapp is outlined in Figure 1 below.

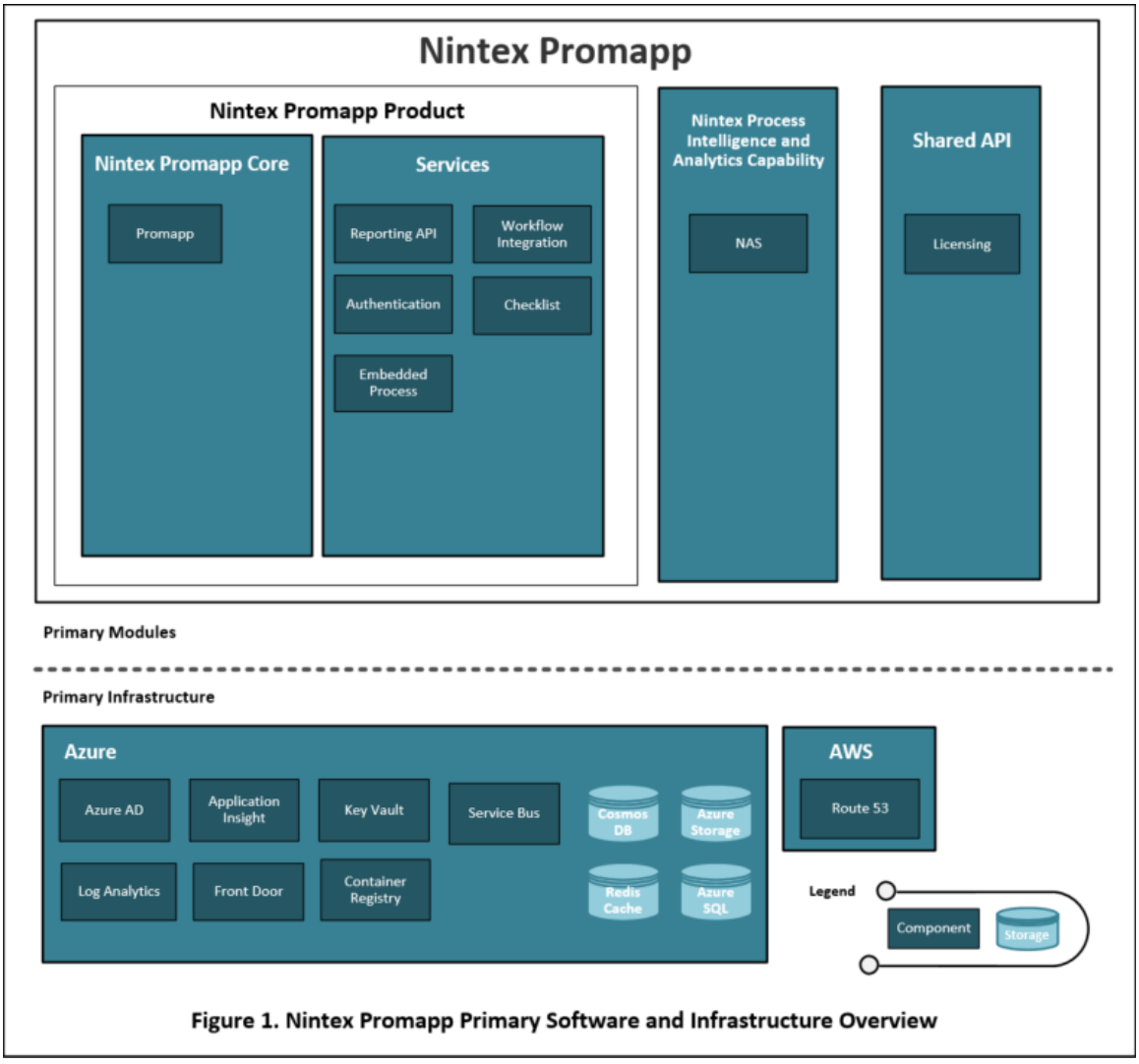

FIGURE 1. NINTEX PROMAPP SOFTWARE AND INFRASTRUCTURE OVERVIEW

2. Infrastructure

Nintex Promapp is based on a multi-tenanted, multi-user software-as-a-service (SaaS), hosted in Microsoft Azure (Azure). See Figure 1.

ACCESS CONTROL

Privileged 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 domain 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.

PLATFORM-AS-A-SERVICE (PAAS) ARCHITECTURE

Nintex Promapp runs on PaaS services within the Microsoft Azure data centers in four distinct geographical jurisdictions (Australia, U.S., Europe, and Canada). 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 Promapp is a monolith (PromappCore), 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 Promapp 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 Promapp production infrastructure is restricted via Microsoft Azure Virtual Network technology, which restricts access to Azure resources from public Internet Protocol (IP) addresses. Nintex Promapp web services are made available to the public through a single entry point to enforce consistent centralized control of routing, firewall, and Transport Layer Security (TLS) connections.

EXTERNAL SERVICES

MICROSOFT AZURE

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

- *Storage Technologies:* Azure SQL, Blob Storage, Cosmos DB, Redis Cache
- *Computing Technologies:* App Services, Functions, Logic Apps
- *Networking Technologies:* Virtual Networks, Frontdoor, Web Application Firewall, Application Gateway, Network Security Groups
- *Integration Technologies:* Service Bus
- *Search Technologies:* Cognitive Search
- *Management Technologies:* Application Insights, Log Analytics, Identity & Security, Azure Active Directory, Key Vault, and Security Center

AMAZON WEB SERVICES

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

INTEGRATION

Nintex Promapp integrates with the third-party email provider, SendGrid. This service is only used to send emails and not receive. Typically emails are sent to inform users of process changes and process approvals that they need to act upon.

Videos uploaded to Nintex Promapp 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 Promapp's Azure Blob Storage. Zencoder does not store the video content.

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

AUTHENTICATION

Users authenticate directly with their Nintex Promapp 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 Promapp tenancy with a Security Assertion Markup Language (SAML)-compliant Identity Provider to allow management of users to be handled outside of the Nintex Promapp tenancy if desired and provide users with Single Sign-On to their tenancy.

APPLICATION MONITORING AND ANALYTICS

Nintex Promapp 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 Promapp.

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

There are several software safeguards implemented for Nintex Promapp. 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.

PROMAPP CORE

The majority of Nintex Promapp'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.

Promapp 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

A number of microservices extend the functionality provided by the Promapp 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 Promapp query the Search microservice, which retrieves the results from the Azure Cognitive Search service.

CHECKLIST

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

REPORTING

Nintex Promapp 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 Jira to track work items and Microsoft Azure DevOps for building and deploying code to the development, test, staging, and production environments. 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
Research and Development	Staff responsible for researching and developing key innovations to advance the Nintex platform technologies, including overall product strategy and the development of a product roadmap.
Operations, Practices & Security	Staff responsible for managing operations, security, and quality management.
Customer Success & Support	Staff responsible for providing timely technical support to customers and ensuring customers maintain a positive, productive experience with the Nintex brand.
Marketing	Staff responsible for promoting the Company and communicating a clear, consistent brand across all channels.
Sales	Staff responsible for sales, 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

Nintex Promapp (see Figure 1) 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 Promapp and services (see Figure 1) transmit all communication via TLS, using a certificate from a well-known certificate provider.

Nintex Promapp pushes data to the Nintex Analytic Service (see Figure 1), 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 Promapp uses Azure storage technologies to process and store data, including but not limited to:

- First and last names, email address of users, their roles within Nintex Promapp, 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

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 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. 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 Promapp®). 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.

C. Complementary User Entity Controls

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

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

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

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

MOSSADAMS