Nintex Platform Security, Privacy & Organizational Overview

Version 1.7 - Published Thursday, October 12, 2023

nintex

nintex

Table of contents

Overview

Thousands of companies around the world benefit from the Nintex Process Platform. As part of our mission to provide the leading enterprise process management and automation capabilities to customers, Nintex is committed to maintaining the security and reliability of all its cloud-based capabilities. The purpose of this document is to provide a high-level overview of the Nintex Process Platform security posture and organizational processes.

Nintex Process Platform cloud-based capabilities covered by this document are the following Software as a Service (SaaS) applications:

- Nintex Automation Cloud
- Nintex Workflow for Office 365
- Nintex Forms for Office 365
- Nintex DocGen for Salesforce
- Nintex Process Manager
- Nintex Insights
- Nintex eSign

Security

Nintex has an internal Security Team responsible for the overall security of the Nintex Process Platform. This responsibility includes working with the Governance Risk and Compliance (GRC) group in developing company-wide security policies and guidelines, performing risk assessments, adherence to compliance initiatives, security related education and identifying the technical, administrative, or physical controls that should be in place to support the mission of information security.

The Nintex GRC group is represented by all major areas of Nintex and is responsible for defining the policies and guidelines required to protect the confidentiality and integrity of customer data and ensuring the availability of Nintex cloud-based capabilities in line with the intentions set forth in this document.

Nintex employs a ‘defense in depth’ approach to implementing security, using available mechanisms and controls to address Confidentiality, Integrity and Availability in the various layers of the platform and infrastructure. This minimizes potential attack vectors by creating multiple layers of defense and adheres to security best practices.

Product teams follow company defined Secure SDLC Guidelines and must adhere to strict data-handling guidelines when building new applications, features, and services on the Nintex Process Platform. Nintex Product teams also conduct regular risk assessments, threat modeling, and compliance reviews to ensure application security adherence.

Compliance

SOC and ISO reports

Nintex is committed to maintaining the security of our products. Our System and Organization Controls (SOC) 2 and 3 and ISO reports provide assurances that there are controls in place that protect your data. Nintex has SOC 2 Type 2 and SOC 3 reports that support Nintex Automation Cloud, Nintex Process Manager, Nintex DocGen for Salesforce, and Nintex eSign services. To request a confidential copy of a report, email security@nintex.com.

FedRAMP

Nintex DocGen for Salesforce has a Federal Risk and Authorization Management Program (FedRAMP) Moderate Authorization. The U.S. government-wide program provides a standard approach for assessing, authorizing and continuous monitoring of cloud-based products and services. The Authorization allows government agencies to realize the benefits of Nintex DocGen for Salesforce. For more information, visit the FedRAMP Marketplace.

Availability

Platform hosting providers

The Nintex Process Platform utilizes Microsoft Azure to host its cloud-based capabilities. Information on the Microsoft Azure Platform can be found in the Microsoft Azure Security, Privacy, and Compliance Requirements.

Shared operational responsibilities

Nintex has a Security Team that is responsible for security at Nintex, including application security. Security is a shared responsibility between Nintex and its hosting provider, Microsoft Azure. Microsoft Azure is responsible for the security of their platforms, including middleware, the servers, and physical security within their data centers.

Customer acceptable use

Shared responsibility also extends to our customers; we trust our customers to use the Nintex Process Platform responsibly. The Nintex Customer Use Policy containing information regarding these responsibilities is available on our Legal page.

Resilience / redundancy

The Nintex Process Platform capabilities are built using a scalable cloud architecture. Nintex continually monitors overall platform performance and when required, scales based on need. Where applicable, we leverage auto-scaling and manual provisioning tailored to the requirements of each Nintex capability. Load balancers are utilized to distribute network and application traffic across multiple servers within a region to increase capacity; queuing and caching are also used to enhance the reliability of services.

Scheduled maintenance

Nintex periodically performs scheduled maintenance. These maintenance periods are typically conducted during weekends and/or outside regional business hours, wherever possible.

Nintex endeavours to minimize the disruption of any maintenance windows or scheduled upgrades and notifies customers in advance (via an externally facing Nintex status page) of any expected and/or significant unavailability or down-time impacts.

Uptime

Nintex uses a range of automated tools to monitor service availability and responsiveness. In the event a service is operating outside of expected thresholds, alerts are triggered and sent via PagerDuty to the relevant teams for investigation. Nintex aims to provide 99.99% availability across all Nintex Process Platform capabilities.

Capacity management

Nintex undertakes proactive steps to maintain sufficient capacity across all Nintex Process Platform capabilities. This includes monitoring the applicable infrastructure to determine that no more than 80% of resources are in use. This allows adequate capacity to support new customers and/or sudden increases in load or storage demands. Overall capacity is increased automatically wherever possible.

Notifications

Nintex provides an externally facing Nintex status page to customers with details on scheduled maintenance activities and current and historical service interruptions. Customers can subscribe to email notifications from this page to be notified of changes to the Nintex Process Platform operational status.

Monitoring and logging

The Nintex Process Platform utilizes a variety of monitoring and analysis tools, including Microsoft Azure and other third-party services. These services provide application and system monitoring, usage statistics, security application event logs, system diagnostics, performance, and page-level statistics for troubleshooting and improvement.

Technical teams are alerted of any conditions outside defined, acceptable parameters.

Access to logs are restricted based on roles within the organization.

Nintex has managed detection and response capabilities established. Security events from product and corporate infrastructure are centrally logged and monitored by the security operation center 24x7.

Security logs are retained for minimum 1 year, with all other logs retained for 90 days.

Data management

Nintex has policies and guidelines for classifying and handling all customer data processed by the Nintex Process Platform capabilities. All Nintex staff involved in handling data are trained on their responsibilities and tested on their knowledge prior to being given access to this data (see the "Training" on page 12 section).

For more detailed information on data flows in Nintex Process Platform services, please refer to the Data Journey Diagram, Trust Boundaries Diagram, and Trust Boundaries Overview documents. For a copy of these documents, contact Nintex Sales. Nintex cloud-based capabilities operate using the following data classifications:

	Secrets *(Tier 1A)*	**PII** *(Tier 1B)*	**Confidential data** *(Tier 2)*	**Public data** *(Tier 3)*
Examples (non-exhaustive)	• *Passwords* • *Signing certificates* • *Encryption keys* • *API secrets*	• *Customer first and last name* • *Customer email address* • *Financial or medical profiles*	• *Tenant ID* • *Company name* • *SharePoint locations* • *Workflow statistics* • *Application and customer telemetry data*	• *Branding details* • *Public product blogs* • *Press releases* • *Public websites*

Data privacy – Personal data

Customers are in sole control of the data entered into the Nintex Process Platform and are responsible for determining whether their data security requirements and obligations under any applicable regulatory framework(s) are being met through use of the Nintex Process Platform. Use of the Nintex Process Platform does not require any sensitive Personal Data. Nintex does not use any Personal Data stored in Nintex applications or services other than for the express purpose of supplying the related service of the Nintex Process Platform to the customer, at the customer's direction.

Nintex self-certifies its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks for data transfers subject to the GDPR. Upon request, Nintex can provide customers with a Data Processing Agreement. For more details, see the Nintex Privacy Policy.

Data security

Nintex maintains a high-level of data security across all cloud-based capabilities within the Nintex Process Platform. Nintex focuses on protecting customer data and content via its security policies, guidelines, product, and organizational controls and by internally conducted risk assessments. All policies, guidelines, and controls are reviewed at least on an annual basis by the Nintex Security Team and GRC, and final approval is given by the Information Security Officer.

Nintex product teams are trained on and are required to follow our security policies and guidelines which include topics such as; data handling, secure software development, cryptography, change and release management, logging and monitoring, creating and storing passwords, and managing vulnerabilities. The information in these policies and guidelines help Nintex product teams standardize and enhance their software development capabilities. Moreover, these policies and guidelines include protections for Open Web Application Security Project (OWASP) Top 10 security flaws, recommendations for avoiding cloud security threats, reviewing data flows through threat modeling processes, performing static vulnerability scans (via Veracode) before each release, and conducting penetration tests via third-party vendors every year. Guidelines are regularly reviewed to reflect the current threat landscape and known vulnerabilities.

Customers retain ownership of, and responsibility for, the data and other content they enter while designing and publishing Nintex Process Platform capabilities. Additional information regarding these obligations is available on our Legal page.

Platform access control

Access to the Nintex process platform 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, and for additional security multifactor authentication, is also required to log into the platform.

Development teams have read-only access to production level diagnostic tools for troubleshooting and improvements.

Platform hosting regions

Nintex leverages multiple regions for hosting the Nintex Process Platform capabilities. Nintex Process Platform capabilities are available in the following regions:

	United States of America	European Union	Canada	Japan	Australia	United Kingdom	United Arab Emirates	Singapore
Nintex Automation Cloud	✓	✓	✓		✓	✓		✓
Nintex Workflow for Office 365	✓	✓		✓	✓			
Nintex Insights	✓	✓	✓	✓	✓	✓		
Nintex DocGen for Salesforce	✓	✓	✓		✓			
Nintex Process Manager	✓	✓	✓		✓		✓	
Nintex eSign	✓	✓	✓		✓			

Encryption

Nintex has Cryptography Guidelines that provide a framework for the proper use of cryptography in Nintex Process Platform capabilities, as well as guidance for software development where there may be a choice of available implementation functions such as transport layer security, symmetric and asymmetric algorithms, and hash function requirements.

Refer to the Data Journey Diagram, Trust Boundaries Diagram, and Trust Boundaries Overview documents for the further detail on specific Nintex Process Platform capability encryption. For a copy of these documents, contact Nintex Sales.

Backups

Nintex performs environment configuration and data backups with a rolling 90-day retention period where required as many capabilities are transient in nature.

Backups are regionally geo-replicated and encrypted at rest.

Change control processes

Nintex has Enterprise Change Management guidelines that provide direction and support for performing consistent production level activities for routine changes, scheduled changes, and emergency changes. The guidelines step through planning the change, approving/rejecting the change, implementing the change, and any rollback. Production releases are performed via controlled pipelines through both testing and staging environments.

Nintex secure application development

Software development at Nintex follows the framework described in the Nintex Secure Software Development Lifecycle (SDLC) Guidelines. These guidelines outline how Nintex Product Teams write secure code that helps protect customer data while supporting the identification of threats and vulnerabilities, and managing potential mitigation activities.

Nintex has dedicated product teams that include developers, testers, user experience designers, and DevOps engineers who work with Product Management, Quality Assurance, and Technical Content resources to produce quality Nintex Process Platform cloud-based capabilities. In addition, the Nintex Security Team works proactively with product teams to implement and maintain Nintex security standards, facilitating threat modeling reviews and managing internal and external risk and vulnerability assessments.

Static vulnerability scans (via Veracode) are performed prior to each release to limit the potential exploitation of Nintex code. All Nintex cloud-based capabilities also undergo third party penetration tests on an annual basis. All Nintex developers are also required to participate in interactive web-based Cybersecurity training for software engineers every year to maintain and enhance their skills in writing secure code.

Business Continuity

Nintex has an overarching Business Continuity Management (BCM) Plan for internal operations. The plan establishes the Nintex BCM function and outlines requirements for the response to, and recovery of, all critical business processes and technology (e.g., physical hardware, business applications, and internal data) in the event of an unplanned business disruption to any portion of Nintex's normal operations.

Disaster recovery

Nintex views availability and disaster recovery through a broader lens of service reliability and resilience, for which we employ internal processes to systematically address. This approach addresses a range of failure modes, particularly those that are typical in cloud environments (e.g., a failure of one component, a partial outage of a specific service, a regional network slow down, or an unexpected peak in traffic).

For each Nintex cloud capability, critical and non-critical dependencies are identified (including platform components, third-party integration services, reporting API services, and auxiliary services) and recovery point objective (RPO) and recovery time objective (RTO) targets are determined and set (generally 60 minutes). Procedures (golden paths) are then created to meet the specified RTO and RPO targets. These golden paths include recommended configurations for reliability and resilience, as well as best practices for utilizing configured resiliency features during an incident.

Any resilience gaps identified which may prevent achieving the RTO and RPO targets are logged and tracked to resolution through our application lifecycle management (ALM) tool. These internal processes ensure Nintex maintains both a detailed and broad assessment of our overall platform resilience.

Nintex also derives substantial benefits from its close partnership with Microsoft and from the reliability that Azure and Microsoft-approved architecture patterns provide.

To manage a broader outage, Nintex has an overarching Disaster Recovery Plan (DRP) that describes team structure, roles and responsibilities, activation criteria, communication expectations, and the overall process, which involves:

- Escalation of major production level incidents (that go beyond a single-source fix or may have a cause for a greater outage)
- Damage and impact assessment / determine recovery priorities
- Formation of the Disaster Recovery (DR) Team, review of DRP activation criteria
- Escalation to the Crisis Management Team (CMT) for a disaster declaration
- Following a disaster declaration, notification to specific recovery teams to activate their runbooks
- Monitoring and effectiveness assessment of recovery activities
- Communication activities between the Disaster Recovery Lead and the Product Disaster Recovery Team
- Recovery acceptance testing
- Post recovery activities
- DR Maintenance

Incident management

Nintex has an Incident Response Plan in place for all cloud-based Platform capabilities. The plan describes team structure, roles and responsibilities, activation criteria, communication expectations, and the overall process, which involves:

- Discovery
- Containment
- Investigation
- Communication
- Mitigation
- Review

Threat and vulnerability management

Nintex has a Vulnerability Management Policy and a Vulnerability Management Guidelines document in place which includes processes for scanning endpoint devices, validation of vulnerabilities, and remediation timeframes.

Nintex product teams follow guidelines for the Threat Modeling of cloud-based Platform capabilities, including the creation of Data Flow Diagrams (DFD) used to identify and complete the analysis of potential threats in the system.

Threat monitoring

Nintex collects and consolidates log events and flow data from devices, endpoints, and applications on the network using a Security Information and Event Management (SIEM) system. The SIEM is monitored 24x7x365 by an external Managed Security Solution Provider (MSSP), who performs initial investigations of any detected issues/anomalies and immediately notifies Nintex according to pre-defined escalation procedures.

Patch management

Nintex has a Patch Management Policy that outlines the processes that ensure Nintex information systems, including applications and software, are patched in a timely manner to reduce or prevent the possibility of unwanted intrusion or exploitation from threats and open vulnerabilities. The Nintex hosting providers are responsible for any Infrastructure as a service (IAAS) component patching.

Physical security

Platform hosting providers

The Nintex Process Platform utilizes Microsoft Azure to host its cloud service. Information on the Microsoft Azure Platform can be found in the Microsoft Azure Security, Privacy, and Compliance Requirements.

Nintex corporate offices

Nintex offices are located in fit-for-purpose buildings with building access via key card only. Visitors must sign in and sign out and are accompanied by an employee when onsite. No customer data is hosted within Nintex offices.

Support

Nintex Support is available at varying levels up to 24x7 depending on the support package chosen. Further details can be reviewed at Nintex Support.

Nintex provides an externally facing Nintex status page to customers. This site provides details on planned maintenance activities and current and historical service interruptions. Customers can subscribe to email notifications from this page to be notified of changes to the Nintex Process Platform operational status.

Employees

How we recruit

Using a tool called Greenhouse, the recruitment process at Nintex is consistent and thoroughly documented. The same process supports both permanent and temporary (contractor) resource hiring.

Applicants are evaluated against role requirements and progress through several rounds of interviews:

- Telephone/video-call pre-screening interview based on essential criteria
- Technical tests (if applicable to the role)
- Technical interview (if applicable to the role)
- Hiring Manager interview
- Team Fit interview with one or more members of the relevant team
- Additional interview/s with senior manager / human resources (if applicable)

Nintex conducts background checks after a candidate has been offered a role. Background checks are performed as allowed by local law, typically involving two or more references as well as an employment verification from the candidate's previous employer.

Individuals seeking employment at Nintex are considered without regards to race, color, religion, national origin, age, sex, marital status, ancestry, physical or mental disability, veteran status, gender identity, or sexual orientation. Where applicable, Nintex participates in E-Verify, and is an equal opportunity employer.

Accounts setup and role changes

Employee access to Nintex systems is granted based on the employee's role. Nintex follows the Principle of Least Privilege (PoLP), where users can only access the systems and data that contain the information that is required to perform their duties.

Access is updated in a timely manner when employees change roles or leave the company. An audit log is kept detailing any requests for access changes, and the actions that are performed to grant or deny this access.

Training

Nintex Learning Central is available to all Nintex employees (both permanent and temporary resources). There are two virtual campuses:

- *Career Development Campus*: Training resources to support career development via LinkedIn Learning
- *Process Platform Campus*: On-demand training for Nintex technologies and required training around security

In addition, Nintex provides mandatory annual security awareness training via Skilljar, the Nintex Learning Management System (LMS). This provides employees the knowledge and tools that maintain the safety and integrity of the Nintex IT infrastructure, cloud-based capabilities, data network, intellectual property, and physical locations. The LMS tracks who has completed the training and provides a quiz at the end of each module (e.g., GDPR Overview, Mobile Device Security, Physical Security, PII in Action, Safer Web Browsing, Safe Social Networks, Social Engineering, etc.). This training (new/different curriculum every year) is required for all new hires as part of the on-boarding process and conducted on an annual basis for all existing employees.

Termination

When an employee's contract is terminated (voluntarily or involuntarily), the Nintex Human Resources department initiates an automated off-boarding process which revokes access to all systems, notifies applicable employees to action off-boarding tasks such as return of equipment, return of access cards, arranging for an exit interview, signing applicable paperwork, etc.

Additional Resources

Nintex Help Documentation

Nintex Website

Nintex Community

Nintex Leaning Central

Nintex YouTube Channel