NINTEX USA, INC.

ASSURESIGN E-SIGNATURE SOFTWARE AS A SERVICE APPLICATION SOC 3 RELEVANT TO SECURITY AND AVAILABILITY

For the Period January 1, 2022 to December 31, 2022

Cherry Bekaert LLP

Your Guide Forward

NINTEX USA, INC.
TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

Cherry Bekaert LLP
Your Guide Forward

Cherry Bekaert LLP
Your Guide Forward

Independent Service Auditor's Report

Nintex USA, Inc.
Bellevue, Washington

Scope

We have examined Nintex USA, Inc.'s ("Nintex" or the "Company") assertion titled "Managements Assertion" ("Assertion") that the controls within Nintex's AssureSign e-Signature as a Service Application ("System") were effective throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that Nintex's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*..

Nintex uses subservice organizations to provide physical security, infrastructure and environmental controls related to infrastructure hosting and application authentication controls in support of the System. The accompanying assertion and the description indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nintex, to achieve Nintex's service commitments and system requirements based on the applicable trust services criteria. The description includes the types of complementary subservice organization controls assumed in the design of Nintex's controls. The description does not disclose the actual controls at the subservice organizations. 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 accompanying assertion and the description indicate that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nintex, to achieve Nintex's service commitments and system requirements based on the applicable trust services criteria. The description presents the complementary user entity controls assumed in the design of Nintex's controls. 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 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's service commitments and system requirements were achieved. Nintex has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Nintex is responsible for selecting and identifying in its assertion, the applicable trust service 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, is fairly stated in all material respects. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 Nintex's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Nintex'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's service commitments and system requirements based on the applicable trust services criteria.

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

We are required to be independent of Nintex and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement.

Our examination was not conducted for the purpose of evaluating Nintex's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on Nintex's cybersecurity risk management program.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error, fraud, targeted social engineering attacks, advanced persistent threats, third-party control deficiencies, 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. Furthermore, projections of any evaluation of effectiveness to future periods are 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's AssureSign e-Signature Software as a Service Application were effective throughout the period January 1, 2022 to December 31, 2022 if complementary subservice organization controls and complementary user entity controls contemplated in the design of Nintex's controls operated effectively, to provide reasonable assurance that Nintex's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

Cherry Bekaert LLP

West Warwick, Rhode Island
March 7, 2023

II. MANAGEMENT'S ASSERTION

Cherry Bekaert LLP
Your Guide Forward

Management's Assertion

We are responsible for designing, implementing, operating and maintaining effective controls within Nintex USA, Inc.'s ("Nintex") AssureSign e-Signature Software as a Service Application ("System") throughout the period January 1, 2022 to December 31, 2022 to provide reasonable assurance that Nintex's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the System is attached 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 January 1, 2022 to December 31, 2022 to provide reasonable assurance that Nintex's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.. Nintex'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 principle service commitments and system requirements related to the applicable trust services criteria are presented in the description.

Nintex uses subservice organizations to provide physical security, infrastructure and environmental controls related to infrastructure hosting and application authentication controls in support of the System. This assertion and the description indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nintex, to achieve Nintex'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's controls. The description does not disclose the actual controls at the subservice organizations.

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error, fraud, targeted social engineering attacks, advanced persistent threats, third-party control deficiencies, 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. Furthermore, projections of any evaluation of effectiveness to future periods are 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.

We assert that the controls within the System were effective throughout the period January 1, 2022, to December 31, 2022 to provide reasonable assurance that Nintex's service commitments and system requirements were achieved based on the applicable trust services criteria.

Electronically Signed 2023-03-31 19:29:23 UTC - 71.197.165.197

Justin Donato

Nintex AssureSign® a744e19b-aa41-4a43-9ab6-afd3016d07ba

Justin Donato
VP, Security & Compliance (Information Security Officer)

T +1 425 324 2400 F +1 425 458 0105 | nintex.com

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

III. MANAGEMENT'S DESCRIPTION OF THE ASSURESIGN E-SIGNATURE SOFTWARE AS A SERVICE APPLICATION THROUGHOUT THE PERIOD JANUARY 1, 2022 TO DECEMBER 31, 2022

Cherry Bekaert LLP
Your Guide Forward

Service Type

Nintex USA, Inc.'s AssureSign Software-as-a-Service (SaaS) application provides software to enable obtaining electronic signatures on documents; primarily through cloud hosted AssureSign eSignature SaaS Application, and through in-house installations of its web software. AssureSign was initially founded as an offshoot of Third-Party Verification, Inc., established in 1999, whose primary business was performing FCC-mandated third-party verifications for telephone local number portability. The AssureSign product was initially developed to expand its electronic agreement methodology to other business verticals.

The AssureSign SaaS application is a web-based tool that provides the following services:

- Secure application programming interface (API) available to clients
- Administration portal
- Signing interface
- Back-end systems

The AssureSign SaaS application is a large-scale, role-based workflow engine allowing for multiple points of entry for administrators and signers. Administrators and signers are granted access to specific areas of the web user interface based on their role within an organization, or their role for a given signing scenario. Privileges are also granted for application access via API communication. Data and documents are encrypted within the AssureSign SaaS environment, and decrypted for download, as requested by customers, over encrypted web channels.

AssureSign SaaS application client users are defined as users who have contracted with Nintex AssureSign to use the AssureSign SaaS application. Client users are segregated from signatories who use the signing portal of the software without access to the password-protected administration portal.

Scope

The scope of the report is limited to the AssureSign SaaS application. On-premises solutions, which may be unique to a customer and are dependent upon the customer's infrastructure, are excluded from the scope of the report.

The AssureSign SaaS application is hosted on Microsoft's Azure cloud computing platform at data centers distributed across diverse geographic locations in the United States, Canada, Europe, and Australia as described in the **System Components** section. Services provided by Microsoft Azure are excluded from the scope of the report.

The Nintex AssureSign corporate network is completely isolated from the AssureSign SaaS application production environment and is excluded from the scope of this assessment. Other items excluded from scope are as follows:

- Configurations unique to individual companies or clients
- Integration with client applications

- Application access via APIs, including DocumentNOW and DocumentTRAK
- Third parties used for transactional email and/or SMS message delivery

Subservice Providers

Subservice providers are excluded from the scope of this assessment. Nintex AssureSign oversees and monitors relationships with third parties to ensure SLAs are met. Below is a description of the applicable subservice providers and the applicability considerations for the report's intended audience.

Microsoft Corporation

Critical Services

- Microsoft Cloud Infrastructure and Operations (MCIO)
- Microsoft Azure Service System

Microsoft Azure is cloud computing platform and infrastructure provided by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters.

SendGrid

Critical Services

- Third-party email services

Nintex AssureSign utilizes third-party email services, such as SendGrid to send documents for electronic signatures and for providing communication between signers. Signers access documents through email messages to review and provide signatures.

IDology

Non-Critical Services

- Third-party knowledge-based identity verification

The IDology service can be enabled in the AssureSign SaaS application to require an additional knowledge-based layer of identity verification.

System Components

Infrastructure

The AssureSign SaaS application is an ASP.NET application running in Microsoft Azure Cloud Services instances. Dedicated external IP addresses are assigned to 6 production instances:

- Azure West US datacenter
- Azure East US datacenter
- Azure Canada Central datacenter
- Azure West Europe datacenter
- Azure Australia East datacenter
- Azure Australia West datacenter

Each instance:

- Runs a virtual web farm in which additional instances of virtual machines, based on a predefined operating environment image with application included, may be automatically added or on demand.
- Sits behind Azure firewall services allowing for definition and monitoring of specific TCP/IP port endpoints.
- Is driven by a separately stored virtual premium-instance Azure database, residing in the same Azure datacenter as the web environment for performance purposes. This instance is separately firewalled to allow communications from specific IP addresses and ports only.
- Is assigned a specific Azure Binary Large Object (BLOB) storage account for document and image storage related to documents signed on the environment.
- Is assigned a separate encryption domain that houses an isolated application and database used to drive encryption and decryption required by the AssureSign SaaS application instance.
- Is assigned a key vault that contains digital certificates for signing documents. This key vault is configured to support a primary AssureSign instance and serve as a secondary instance in the event of failures of another site's primary key vault instance that is used for signing documents.

Software

The core application supporting the AssureSign SaaS Application is a multi-user web-based application that provides the following services:

- A secure application programming interface (API) available to clients that allows for:
    - Upload of documents in various electronic formats that require signature
    - Querying of document status during and after electronic signing

  - Remote manipulation of document workflow and notifications through on-demand requests for actions
  - Download of completed documents
- An administrative portal allowing for:
  - Client creation, deletion, and management of user accounts
  - Client creation, deletion and management of sub-accounts allowing for unique business rules per account
  - Security controls allowing for client designed rules regarding access and the operation of the software
  - Control of the requirements for the client account with respect to signing, including:
    - Management of rules regarding signing passwords
    - Management of knowledge-based authentication processes for signing
    - Branding
    - Management of supplemental display of customer specific provisions and legal statements
  - Design of document signing templates
  - Design of emails sent on behalf of the client
  - Design of integration with external electronic systems
  - Reporting
- A signing interface, that consists of a browser-agnostic portal for signatories to:
  - Agree to sign electronically
  - Agree to any additional terms implemented by clients who have requested the document be signed by the signatory
  - Access required privacy terms and general terms of use applicable to non-customer signatories (signers who are not paid customers of AssureSign)
  - Access additional documents that may have been provided by clients for review by the signatory
  - View and download the unsigned document
  - Create and apply electronic signatures in accordance with appropriate regulations
  - Upload images and other electronic file attachments that clients have indicated must be solicited
  - Submit all signatures to be applied
  - Download the completed document
- Back-end systems, including:
  - Databases
  - Signed and unsigned document storage
  - Encryption processes used to encrypt data and documents
  - Decryption processes used to decrypt data and documents for download or for external communications

- Application of all signature elements submitted by signatories
- Recording of evidentiary information regarding signing, including IP addresses of signers, information regarding the signers' browser, signers' geo-location information
- Email processing of notifications that have been designed by clients to occur at various triggering events in the life of a document
- Key vaults used to store certificates issues to sign AssureSign documents and which perform signing processes invoked by the core web servers.
- Communications of web notifications, including passing of signed documents, to client internet addresses, which may include:
  - Secured website services, such as via raw POST operations or via SOAP web methods
  - FTP and SFTP servers
  - Email
  - Short Message Service (SMS) text message

The AssureSign SaaS application system is designed to obtain electronic signatures on any type of electronic document where an electronic signature is legal. The software allows customers to upload their own documents and workflow to be signed within the AssureSign SaaS application signing infrastructure.

Clients could potentially apply or solicit signers of their documents to apply private or sensitive information to documents during the online signing session. The AssureSign SaaS application provides protections to ensure the privacy of this information is maintained.

People

Due to the size of the organization, certain staff members serve in multiple roles. Personnel involved in the operation and use of the system function in the following areas.

Software Engineering

The Software engineering staff is responsible for:

- Developing the AssureSign SaaS application
- Developing and maintaining the AssureSign SaaS databases
- Implementing releases of the AssureSign SaaS application to production SaaS instances
- Developing and supporting integration tools that allow for AssureSign API services to be accessed from miscellaneous desktop and mobile platforms
- Maintaining the SDLC schedule timeline of feature requests and bug fixes
- Developing and maintaining internal administration tools used by Customer Success and Accounting
- Providing second tier support for client technical issues.

Separate roles exist within Software Engineering, such that only senior engineers can access and update the encryption services.

Policy and processes are implemented for Software Engineering through the Senior Director of Engineering. This role oversees reviews of the development environment, ensures targets are met for training, implements policy ensuring day to day development operations occur in a secure manner, ensures compliance with code review processes, and conducts staff scrum meetings.

Development of automated testing of scripted scenarios is overseen by the Software Engineering staff due to its integration into the automated build process: Test scripts are included in Visual Studio solutions that are built and invoked during the build process, and these scripts are run on a triggered basis on check-ins to the version control system.

Quality Assurance

Quality Assurance (QA) exists in the same organizational reporting structure as Software Engineering. QA must sign off on the testing of AssureSign SaaS application releases, indicating what can be released with what level of testing. The QA handoff must occur before an Executive level sign-off for final release of a build into production environments. QA processes may occur over several release cycles for larger architectures or features, with incremental testing occurring as specific sub-tasks are completed, and full path testing being performed prior to overall release. Since much of the AssureSign SaaS application system is exposed through web components, QA uses third party web-testing tools such as BrowserStack to ensure the systems works across all browsers.

Nintex Information Technology

Nintex Information Technology is responsible for the internal network operations, which is completely segregated from the AssureSign SaaS Application environment and not included in the scope of the assessment.

Nintex Security Practice Team

The Nintex Security Practice Team is responsible for ensuring secure practices are implemented in the software development life cycle (SDLC), as well as developing and implementing the organizational-wide security policy and ensuring compliance through SOC 2 audits. This team is also responsible for implementing, maintaining, and testing the Business Continuity and Disaster Recovery (BC/DR) plan in coordination with Software Engineering.

Customer Success

Members of Customer Success (CS) interact with clients. In the client facing PM role, they may help guide client integration with AssureSign APIs. In addition, they perform the following activities:

- Provide notifications of changes and maintenance
- Serve in an Account Representative role for larger customers, where ongoing application performance reviews or SLA reviews are required

- Serve as first tier support on non-technical questions and account services, escalating to Software Engineering
- Perform non-technical account provisioning and configuration for non-self-signup customers

CS staff do not use the production AssureSign SaaS application for any role where client signer data is exposed. Account provisioning and configuration is performed through administrative tools which grant no access into individual customer transaction data or documents.

Policies and Guidelines

Management has developed and communicated to internal staff procedures to restrict logical access to AssureSign data. In addition, procedures for self-management of security processes and available tools that AssureSign develops for this purpose are made available to clients who access AssureSign systems. Policies and Procedures include:

Security Policies

- Access Management Policy
  The Access Management Policy outlines security practices to prevent unauthorized access to Nintex and customer information systems. It defines the rules necessary to achieve this protection and to ensure secure and reliable operations in accordance with Nintex's business requirements, and in compliance with applicable laws and regulations.
- Asset Management Policy
  The Asset Management Policy outlines requirements for the identification and protection of physical hardware assets connected to Nintex information systems. 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
  The Information Security Policy outlines management direction and support for the Nintex Information Security Program and Policy activities. This Policy defines the necessary rules for security protection, designed to ensure secure and reliable operations in accordance with Nintex business requirements and applicable laws and regulations.
- Password Management Policy
  The Password Management Policy governs password usage of all Nintex employees, contractors, and interns (collectively, "Users"). It helps protect Nintex, Users, vendors, partners, and customers from potential harm caused by a compromised network or system.
- Patch Management Policy

The Patch Management Policy outlines the processes to ensure that 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 open vulnerabilities.

- Security Incident Response Policy
  The Security Incident Response Policy outlines the requirements within the Nintex organization for handling security incidents. The policy describes appropriate responses to incidents that threaten the confidentiality, integrity, and availability of information assets. Together with the Incident Response Guidelines, it establishes an effective incident response program to detect, analyze, prioritize, and handle security incidents.
- Vulnerability Management Policy
  The 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.
- Risk Assessment Policy
- Account Provisioning and Deprovisioning Guidelines
- Cryptography Guidelines
- Data Handling Guidelines
- Data Sanitization Guidelines
- Enterprise Change Management Guidelines
- Enterprise Release Management Guidelines
- Password Guidelines
- Secure SDLC Guidelines
- Security Exception Guidelines
- Security Incident Response Plan
- Security Logging and Monitoring Guidelines
- Threat Modeling Guidelines
- Use of Tier-1 & Tier-2 Data for Testing Guidelines
- Vendor Management Guidelines
- Vendor Security Review Guidelines
- Vulnerability Management Guidelines

Software Engineering Policies

- Build and Continuous Integration Policy
- Code Review Policy

- Remote Debugging and RDP Policy
- SaaS Root Access Policy
- SDLC Policy
- Secure Blob Storage Policy
- Secure Code Training Policy
- Secure Mail Policy
- Secure SQL Access Policy
- Software Engineer Access Privileges Policy
- Software Engineer Password Policy
- Code Review Processes
- Server Hardening Script Processes
- Server Startup Script Processes

Security Best Practices

Security processes and best practices has been created for client users to keep their accounts secure. These best practices are listed on the Nintex Community and include guidelines for:

- Creation of subaccounts
- Creation of users
- Document preferences
- DocumentNOW integration
- DocumentTRAK security
- Manual document and template creation
- Security settings

System Access

Authentication and Authorization

Access to system information is protected by authentication and authorization mechanisms. Two-factor authentication is required for both the Microsoft Azure production and security environments. In addition, Nintex IT personnel can make firewall configuration changes to restrict IP addresses from which SQL access is allowed, with the default value set to deny all.

Account Provisioning and Deprovisioning

Nintex AssureSign maintains a User Account Management Policy that includes the logging of access, ensuring protocols are in place to grant and revoke rights, and granting employees only the specific rights needed to accomplish their jobs. Access rights assigned are reviewed on at least an annual basis.

Application Development and Change Management

Cross-functional, long term *scrum* meetings are held periodically to identify and evaluate system change requests, including the impact on security and availability commitments. The Development Team holds cross functional *sprint* planning meetings every two to three weeks to manage and control the development cycles. Development source code is subjected to processing of automated unit testing scripts and a peer secure code review. Changes must be fully tested and approved by Quality Assurance; a function separate from Development. Prior to release to production, an automated regression testing suite is run against a QA instance containing the release candidate build. In addition to QA approval, changes must receive an Executive level sign-off for final release of a build into production environments. The Build process is scripted, and Developers rotate responsibility for deploying approved builds. Alerts are established to notify subscribed personnel of code check-ins and builds. Each environment built is compiled with security keys unique to the environment for purposes of application encryption and decryption, so that a software build could not be taken and run on a generic platform. Post-deployment validation and testing is performed to help ensure changes function as intended.

Business Continuity and Disaster Recovery

The AssureSign SaaS application production instances are housed in regionally dispersed Microsoft Azure data centers. Nintex AssureSign maintains a fully redundant location for restoration if needed. Microsoft is responsible for maintaining continuity of its services.

The organization has developed a Business Continuity and Disaster Recovery (BC/DR) plan to identify significant areas of organizational risk to the data it maintains and the continued availability of its AssureSign SaaS applications. The BC/DR addresses operating facilities, technology, data, roles, redundancy, and resiliency. The BC/DR identifies key contacts and the responsibilities with respect to the plan are identified. The contact data is updated as needed to ensure the BC/DR contains a complete directory chain of internal plan contacts and roles.

The BC/DR includes an Incident Prevention Plan. This section includes identification of key risks facing the organization. These risks, along with the entire document is considered a live document as it is reviewed on a regular basis and updated according to organizational and technological changes. The incident prevention plan provides a map of components of the organization, including critical technology components, that are subject to negative impacts by the identified risks. Components are itemized to include background information, support contacts, physical location, and internal supporters. Policies, actions, are protections are inventoried to ensure the organizational operating environment considers the prevention and recovery from various incidents outlined in the

list of risks. Known shortcomings, areas where improved controls are desired, and longer-term migrations being done to address risk are also outlined in this section of the document.

A Mitigation Plan is provided and includes a template for escalation as well as a recovery plan. The escalation procedures are tested annually to ensure the viability of internal and external notification processes. The recovery plan, primarily focused on data protection, is tested annually, and updated as needed.

Post incident processes are identified in the Continuity Plan, and specific aspects of the processes of breach notification, client contact list maintenance, SLA notification information, and the preservation of billing and financial information are identified.

Incident Response

Nintex AssureSign maintains an incident management process that involves prioritizing events according to levels of severity. These incidents are submitted to the Nintex AssureSign support staff and a separate management personnel handles each level of severity within a specified resolution timeline.

Data

Nintex AssureSign systems contain data to include:

- System level configuration data
- System configuration data set by clients
- Data provided by clients regarding signers and their documents
- Transactional data obtained during signing from signatories
- Unsigned and signed documents in electronic form
- Export data communicated by workflow processes to customer systems
- Encryption and decryption related data
- Error logs

Data within the Nintex AssureSign systems requiring encryption include:

- Signed and unsigned signatory documents
- Non-text image versions of the documents used for displaying in a web browser
- Document signer related data
- Data used during the signing transaction

Encryption keys, key-encryption keys, and the underlying metadata of the Key Management System (KMS) are not available to be viewed or managed in visible form by non-privileged staff. KMS related data is isolated from all other forms of Nintex AssureSign data. Historical log data required to be present to document KMS activity is isolated in separate databases and storage accounts that may not be managed with employee user accounts used to access other parts of Nintex AssureSign internal systems.

Complementary User Entity Controls

Nintex AssureSign's services were designed with the assumption that certain controls would be implemented by user entities to achieve the applicable Trust Services Criteria. These controls should be in operation at user entities to complement Nintex AssureSign's system of controls. The user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities; other internal controls may be required at user organizations.

Complementary User Entity Controls	Control Criteria
User entities are responsible for promptly reporting any suspected security or availability issues to AssureSign.	CC2.3
User entities are responsible for promptly notifying AssureSign of terminated Administrators.	CC6.2

User Entity Responsibilities

For a user entity to derive the intended benefits of using the services of the service organization, the user entity has certain additional responsibilities related to the system. The following user entity responsibilities have been identified by Nintex in support of the AssureSign SOC 2 examination.

User Entity Responsibilities	Control Criteria
User entities are responsible for establishing and ensuring adherence to internal security policies and procedures.	CC2.3
User entities are responsible for establishing proper controls over use of system IDs and passwords.	CC6.2
User entities are responsible for managing application security within the SaaS application.	CC6.2
User entities are responsible for securing the software and hardware used to access AssureSign.	CC6.2
User entities are responsible for monitoring system upgrade announcements and outage notifications, which may be subscribed to on AssureSign Status.io and monitor on Nintex Help Center.	CC2.3

Complementary Subservice Organization Controls

Nintex AssureSign's services were designed with the assumption that certain controls would be implemented by subservice organizations to achieve the applicable Trust Services Criteria. It is not feasible for the related control criteria to be achieved solely by Nintex AssureSign. Therefore, each user entities internal controls must be evaluated in conjunction with Nintex AssureSign's controls, considering the related complementary subservice organization controls expected to be implemented at the subservice organizations.

Complimentary Subservice Organization Controls	
Microsoft Corporation: Provider of Microsoft Azure and Microsoft Data Centers	
1	Microsoft is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning to the platform services supporting AssureSign.
2	Microsoft is responsible for maintaining controls over protection of the network environment, including hardening and configuration standards for the technical infrastructure, and protecting access to network devices.
3	Microsoft is responsible for providing agent-based infrastructure monitoring within the Azure platform to provide automated detection, logging and alerting of potential unauthorized activity and security events.
4	Microsoft is responsible for maintaining firewalls used to filter network traffic from the Internet and to restrict access to certain resources (Key Management Service, SQL database).
5	Microsoft is responsible for maintaining anti-malware, where enabled, on Azure deployment environment VMs.
6	Microsoft is responsible for automatically applying patches to Guest VMs.
7	Microsoft is responsible for providing a load-based dynamic balancing mechanism, so each Azure environment allows for runtime allocation and de-allocation of web and service processes, providing real-time automatic performance improvement
8	Microsoft is responsible for ensuring controls are implemented to design, develop, implement, operate, maintain, and monitor environmental protections.
9	Microsoft is responsible for performing backups, maintaining a fully redundant infrastructure and for restoring virtual servers and the technical infrastructure in the event of an outage.
10	Microsoft is responsible for maintaining system availability commitments for the Azure infrastructure.
11	Microsoft is responsible for maintaining and monitoring physical security controls.

Complimentary Subservice Organization Controls	
SendGrid: Provider of third-party email services	
1	SendGrid is responsible for providing email services to send documents for electronic signatures and for providing communication between signers.

Complimentary Subservice Organization Controls	
IDology: Provider of knowledge-based identity verification	
1	IDology is responsible for providing an additional "knowledge-based" layer of identity verification, if configured.