Nintex Customer Use Policy

April 2019

Nintex is committed to providing the leading process management and automation platform to its customers. We have created a cloud platform to help you manage, automate, and optimize human-centric, manual, and paper-based business processes. In exchange, we trust our customers ("you") to use the Nintex process management and automation platform (hereinafter the "Service") responsibly.

You agree that you, or anyone else using the Service through you, may not use the Service in a way that:

- Could harm the Service or impair others' use of the Service
- Sends unsolicited communications, promotions or advertisements, or spam
- Abuses referrals or promotions to obtain additional usage rights
- Circumvents your license and entitlement limits (including, but not limited to, Purchased Volume, Employee Plan, Processes, Documents, Users, and/or Viewers)
- Violates the law in any way
- Violates the privacy or infringes the rights of others
- Intentionally distributes malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature, or
- Alters, disables, interferes with, or circumvents any aspect of the Service, including but not limited to security or authentication features of the Service.

Violations of this Policy may result in suspension of your access to the Service. Nintex will suspend your access only to the extent reasonably necessary and will provide reasonable notice before suspension.

For Nintex workflow platform customers, there are no limitations on the number of Design Actions or the Workflow design elements that you may use. For Enterprise Edition customers, there is no limit on the number of mobile workflow applications that may be deployed with Nintex App Studio. However, Nintex has found that certain practices and designs allow for an optimal experience while using the Service. These include avoiding workflow design that creates excessive or indefinite looping and use of high volume automated means to access the service. If Nintex becomes aware that your use of design actions, mobile workflow apps, or your workflow designs are causing performance concerns for you or other Nintex users, you will be contacted to discuss optimizing your use of the Service.

For all customers, if you exceed your entitlement limits, you will be provided notice thereof in the Service. If you continue to exceed your entitlement limits for a period of not less than thirty (30) days after notice thereof, Nintex may suspend your access to the Service with reasonable prior notice. Customers should implement appropriate controls to ensure that only users authorized by the Customer have access to the Service and that no actions are taken by these users which would impact the continued security of the Service.

The Nintex Service was designed under the assumption that certain controls would be implemented by the users of the Service. You should evaluate your internal control structure to determine if the appropriate controls are in place. You are responsible for the following:

- Understanding and complying with your contractual obligations to Nintex
- Immediately notifying Nintex of suspected or confirmed information security breaches, including but not limited to compromised user accounts or passwords
- Developing disaster recovery and business continuity plans that address their ability to use or access the Service
- Protecting end-points to thwart malicious software from entering the Service execution environment
- Notifying Nintex of changes made to technical or administrative contact information in a timely manner
- Designating internal personnel who are authorized to request user additions, deletions, and security level changes
- Managing the user access controls for provisioning and deprovisioning user accounts. This includes enforcement of password policies, management of shared accounts, and authorization approvals
- Restricting administrative privileges to approved need-to-know personnel
- 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
- Understanding and defining data storage requirements
- Securely configuring any EFSS systems or other systems where files are eventually stored
- Managing the confidentiality and integrity of the distribution of authentication tokens used to start component workflows, and
- Managing need-to-know and least privilege when sharing workflows

C**ontact Us**. If you have any questions or suggestions regarding this Policy, please contact Nintex at support@nintex.com.