K2 NEXUS – SERVICE POLICIES

7/14/2020

TABLE OF CONTENTS

1 INTRODUCTION

K2 Nexus is a cloud-based, hosted Platform-as-a-Service (PaaS) offering that provides K2 software and supporting components as a service (the “Service”) which allows K2 customers who prefer a “cloud first” strategy to utilize a cloud-based service, in which software and associated maintenance operations can be licensed as a comprehensive service managed by K2. With K2 Nexus, K2 provides and maintains the platform that enables customers to build applications on K2, without the overhead of setting up, hosting and maintaining K2 environments. The customer does not manage or control the underlying infrastructure (such as network, servers, operating systems, storage or K2 software components), but retains control over the application development cycle and deployed applications.

This document describes the Service as well as policies applicable to the Service and is intended for anyone interested in researching and planning for the Service Offering. The Service is provided under the terms of the K2 Nexus Subscription Agreement (the “Subscription Agreement”), the applicable Order (as defined in the Subscription Agreement) and the policies described within this document. These policies are subject to change at K2's discretion. The Service as ordered by the customer will be governed by the policies in effect at the time the Service was ordered for the period acquired. These policies are reviewed annually and may be revised to incorporate issue resolutions and process improvements.

As used in this document, the terms “Customer,” “Subscriber,” "you" and "your" refer to the individual or entity that has ordered the Service from K2 or an authorized distributor, as applicable.

2 ONBOARDING JOURNEY

This section describes the typical onboarding journey for new customers of the K2 Nexus Service.

1 **Customer Onboarding Session**
The customer and Customer Success Management team complete an onboarding call that details:
- The specifics of the Service.
- The roles on the customer and K2 side that will be involved in coordinating and configuring K2 Nexus for the customer’s identity provider tenant. Additional integration into a customer’s other line-of-business systems can be discussed and coordinated with the Remote Mentoring offering as well.
- Details of the Technical Support system – specifics on how to file a ticket, check on ticket status and how to work with the Support team.
- Details on communication of Service updates from the Service Operations team.
- Details on preferred region deployment of the Service. Available regions are listed in the Service Regions section below.
- General use of the Service.

2 **Core Infrastructure Provisioning**
Service Operations and Datacenter Operations will provision standardized core Service infrastructure in established datacenter locations, at a location agreed with the customer to facilitate data location and latency requirements for the customer’s production K2 Nexus

environment. See the production and non-production environment details in the Included Services section below.

Core service infrastructure setup will include

- The required hardware and virtual servers to operate the service
- Network infrastructure setup and configuration such as firewalls and load balancing
- K2 Nexus database installation and configuration
- K2 Nexus software installation as per best practices
- Installation of quality-of-service monitoring software
- Testing the K2 Production environment by performing base configuration testing
- Disaster Recovery infrastructure setup and configuration
- Service end points and URLs finalization
- Service monitoring setup

3 **Service is made available**
K2 Nexus Service environment(s) available for use by customer's K2 Administrators and Developers.

3 ROLES

There are various roles involved in a Service subscription; use the table below to understand the role definitions.

3.1 CUSTOMER ROLES

Customer Domain Users	Users within the customer's identity provider domain. Consider these the internal end users of the applications built in the K2 environment.
Customer K2 Administrators	Customer resources who maintain the applications and application-specific components on the K2 production and non-production environments.
Customer K2 Helpdesk	Customer resources who provide first-level application support for the applications deployed on the K2 production and non-production environments.
Customer K2 Developers	Customer resources who are responsible for building applications that run on or utilize K2 Nexus environments. These include no-code developers who may build applications with tools like K2 Designer as well as coding-developers who build applications that extend K2 Nexus or interact with K2 Nexus though the available APIs.

Customer Identity Provider Administrators	Customer resources who can administer the customer's identity provider environment.
Customer SharePoint Online Administrators	Customer resources who administer the customer's SharePoint Online environment. NOTE: SharePoint Online is not required to operate K2 Nexus and this role is only required if the customer requires integration into SharePoint Online.
Customer Network Administrators	Customer resources who maintain the customer's network and network infrastructure.

3.2 K2 SERVICE PROVIDER ROLES

K2 Service Account	The identity of the K2 Service Account, the account under which the Service runs.
Service Operations	Service resources who maintain the K2 environment and associated infrastructure and provide support for operational issues.
Customer Success Manager	Service resource who acts as the customer's main liaison and contact person.
Service Onboarding	Service resources who assist during the customer onboarding phase.
Technical Support	K2 Nexus technical support services.
K2 Professional Services	K2 consulting services.
K2	Refers to other, internal K2 roles and operations.
Datacenter Operations	Resources provided by the datacenter provider to maintain aspects like hardware and network infrastructure on the Service infrastructure.
Computer Security Incident Management Team (CSMIT)	Team of Service resources that respond to security threats and breaches.

4 PRE-REQUISITES AND REQUIREMENTS

The following prerequisites and requirements must be satisfied to subscribe to the Service.

- The Service requires the customer provide one of the following to provide authentication of users:
  - An identity provider (IdP) that conforms to the following identity specifications:
    - OpenID Connect
    - System for Cross-domain Identity Management (SCIM) 2.0
  - One of the following Microsoft Azure Active Directory editions:
    - Free
    - Basic
    - Premium P1
    - Premium P2

  It is important for the customer to validate the edition of the identity provider they provide will work for their authentication needs as well as to understand and plan accordingly around the identity provider that is to be incorporated with the Service.

- For customers integrating K2 Nexus with an Azure AD tenant:
  - If a customer is utilizing both on-premises Active Directory (AD) and AAD; the customer's AAD environment must be synchronized with the organization's on-premises AD domain.
  - Customers will be required to deploy the "K2 for Office 365" app into their AAD tenant to facilitate the authentication of users within the Service. The "K2 for Office 365" app requires read-only permissions within a customer's AAD environment.
  - Using a dedicated AAD service account for the K2 integration into AAD is highly recommended.
    - This account should be assigned Global Administration permissions.
    - The Service account must have an allocated mailbox through the appropriate O365 license plan. K2 Nexus administrative notifications, including service status updates and consent expirations, will be sent to this email account. Email forwarding from this account to the K2 Administrators role is highly recommended so that critical notifications are not missed.
  - For customers requiring the ability for the Service to be allowed to create/updated/delete information within AAD, an additional "AAD for K2 Management" app is required to be installed and configured within the AAD tenant; this will require the customer to consent to granting K2 "write" capability within the customer AAD tenant.

- For customers integrating K2 Nexus with a SharePoint Online tenant:
  - An O365 subscription that supports third-party developed apps being deployed into the customer's tenant is required.
  - An O365 subscription that contains SharePoint Online contained within the SKU is required.
  - The account used during the registration of K2 and SharePoint Online must have Global Administrator rights in Office 365, to grant consent between the "K2 for SharePoint" app and SharePoint Online.
  - Site Collection Administrator rights in SharePoint Online are required to add the "K2 for SharePoint" app to the SharePoint Online App Catalog and SharePoint Site Collections.

NOTE **Customers are required to utilize a valid identity provider valid identity provider for authentication and authorization within a K2 Nexus Service subscription. On-premises-based Microsoft Active Directory will not meet the requirements of the Service and can only be utilized if serving as a source for user credentials to be synchronized with given identity providers.**

5 K2 NEXUS SERVICES

A K2 Nexus Service subscription includes several services that, when combined, constitute the Service Offering. The following sections describe the standard included services, excluded services and services that will be available separately.

5.1 INCLUDED SERVICES

Category	Description	Roles involved
On-boarding Services	K2 provides onboarding services to enroll in the Service, available from the on-boarding call with the Customer Success Manager until the Service is made available to the organization.	**K2** • Customer Success Manager • Service Onboarding • Service Operations **Customer** • Customer identity provider administrator • Customer SharePoint Online Administrators (if integrated) • Customer K2 Administrators
Service setup and installation	Core infrastructure provisioning such as application servers, database servers, networking hardware, virtualization, operating systems and applications needed to support the K2 Nexus installation.	**K2** • Service Onboarding • Service Operations

Category	Description	Roles involved
Production K2 Nexus environment	A production environment is made available to all K2 Nexus customers. Customers will access K2 Nexus design, workspace and management tooling via a web-based URL. Customers may request a specific tenant name for their environment during the on-boarding process.	**K2** • Customer Success Manager • Service Onboarding • Service Operations **Customer** • Customer K2 Administrators
Non-production K2 Nexus environment	Customers that require additional non-production environments will work with their Customer Success Manager to coordinate provisioning and accessing such additional non-production environments.	**K2** • Customer Success Manager • Service Onboarding • Service Operations **Customer** • Customer K2 Administrators
Service planned maintenance	Scheduled core infrastructure maintenance such as hardware upgrades, operating system and application version upgrades.	**K2** • Service Operations • Datacenter Operations
Service unplanned maintenance	Unplanned core infrastructure maintenance such as replacement of failed hardware or installation of critical operating systems and application patches.	**K2** • Service Operations • Datacenter Operations
K2 Nexus configuration	Configure the K2 Nexus Service and supporting technologies.	**K2** • Service Operations
Operations Monitoring	Quality-of-service monitoring of infrastructure and K2 to ensure the Service is performing to specification. These metrics are collected and made available to the Service Operations team to make adjustments to the Service as necessary.	**K2** • Service Operations

Category	Description	Roles involved
K2 Nexus Service Health Dashboard	Customers have access to a Service status monitoring webpage. The details of this page will be provided during the customer onboarding process.	**Customer** • K2 Administrators
Standard Backup	Configure and perform automatic backups of the infrastructure and Service-specific databases.	**K2** • Service Operations
High Availability	If necessary, address failures using the appropriate failover mechanism.	**K2** • Service Operations • Datacenter Operations
Recovery	When necessary, restore underlying Service data infrastructure either via a customer request or as the result of an overall disruption in Service.	**K2** • Technical Support • Service Operations **Customer** • K2 Administrators
Disaster Recovery (DR) and Failover testing	Verification that backup is configured correctly and operational by running fail-over and DR tests.	**K2** • Service Operations • Datacenter Operations
Infrastructure and Service environment troubleshooting	Troubleshooting issues in the core infrastructure and Service environment. Customer Application troubleshooting is not included in these services.	**K2** • Technical Support • Service Operations **Customer** • K2 Administrators
Promotion of applications	Ability for the customer to promote Service application elements (SmartForms, Workflows, SmartObjects, Services Definitions) between environments using K2 Package and Deployment tools.	**Customer** • K2 Administrators • K2 Developers
Service security administration	Administer users and permissions for Forms, Workflows and SmartObjects.	**Customer** • K2 Administrators • K2 Developers
Service system administration	Service administration tasks as necessary to address system instability or reliability issues.	**K2** • Service Operations

Category	Description	Roles involved
Service usage	Administer and report on licensed usage.	**K2** • Service Operations **Customer** • K2 Administrators
Reporting	Reporting on Service quality.	**K2** • Service Operations • Customer Success Manager
Requests and tickets	Online system to log requests and support issues.	**K2** • Technical Support **Customer** • K2 Administrators
Technical Support	K2 provides access to K2 support centers and core engineering teams as needed.	**K2** • Technical Support
K2 API Access	All standard, supported K2 Nexus web-based APIs are included in the Service. Customers can reference these APIs when building custom applications to connect to the Service.	**Customer** • K2 Developers
Security monitoring and response	Management and containment of security-related incidents or breaches as described in the Security Incident Response section below.	**K2** • CSMIT
K2 licensing costs	The Service subscription will include specified K2 licenses. Additional charges may apply for additional K2 components and/or services. Customers may acquire additional K2 licenses as user counts or usage increase.	**K2** • Service Operations • Customer Success Manager **Customer** • K2 Administrators

5.2 ADD-ON AND ADDITIONAL COST SERVICES

Services which may incur additional cost include (but are not limited to) the following:

Service	Notes
Troubleshooting	Where K2's troubleshooting exercises repeatedly (more than 3 times) determine that root cause is related to "how-to," non-K2 issues or customer related operational issues, further K2 assistance may be available through K2 professional services.
Customer-initiated data recovery	Customer-initiated requests to restore point-in-time data from a database backup may be requested via a Technical Support Ticket request. The capability to recover data is based upon the Recovery Point Objective policy associated with the customer's Service.
Investigation of impact of data restoration	K2 Nexus typically acts as middleware and interacts between various systems based on workflow tasks, escalations or other mechanisms. Restoration and re-activation of restored workflows might cause unexpected issues, such as duplicated transactions in other systems or re-escalations. As these issues may be solution-specific, K2 professional services can be engaged to investigate the impact of restoring a K2 Nexus database to a specific point in time.
Configuration of additional integration points	K2 professional services can assist in the configuration of integration points and functionality that is not part of the standard onboarding process.
Additional production and non-production environments	Additional instances of production and non-production Service environments are available separately.
Configuration of additional network infrastructure	Customers that desire to connect Service environments to on-premises systems via special network infrastructure (such as VPN) are responsible for obtaining all related network infrastructure and configuration. The Service Operations team will assist in "last mile" connection to the Service. Additional annual Service fees are required to connect the Service environment to such network infrastructure. Customers will be responsible for both the external network infrastructure costs as well as any additions to the base Service infrastructure.

5.3 EXCLUDED SERVICES

Actions which are not provided as part of the Service may include (but are not limited to) the following:

Service	Notes
Identity provider configuration and setup	Service Onboarding will provide requirements, instructions and policies for setting up integration with the customer's identity provider in preparation for Service onboarding. Such IdP changes need to be made by the customer and are not provided as part of the Service.
Application testing	Testing of new or updated customer applications and testing of applications against new versions of K2 software is not included in the Service. K2 software upgrades could have both expected and unintended effects on applications. While K2 continues to invest significantly in testing and QA to minimize impact from upgrades to the Service, ultimately it remains the customer's responsibility to test applications against new version of the Service. See the Change Management section for more information.
Third Party product integration	Integration with any third-party system that is not already included in the Data Integration Options section below is not available within the Service.

5.4 SERVICE REGIONS

The K2 Nexus Service is available to customers that can be accommodated via the following datacenter regions:

Datacenter Region	Support Country Location
US West	United States
US East	United States
US Central	United States
Central Canada	United States
West Europe	United Kingdom South Africa
UK South	United Kingdom South Africa
South Africa North	South Africa
Australia East	Australia

South East Asia	Singapore

NOTE **Customers are responsible for validating that they are able to legally operate in the third-party datacenter regions described above. Customers should also be aware that in some situations both Datacenter Operations and Technical Support may be hosted in a country other than where the datacenter is located.**

6 SERVICE AVAILABILITY

The Service is designed to be available to the customer 24 hours a day, 7 days a week, 365 days a year, except during system maintenance windows, unplanned downtime and as otherwise detailed below.

6.1 OVERALL SERVICE AVAILABILITY

The Service is available when the customer is able to access the Service production environment.

NOTE **The K2 Nexus Service offers customers a 99.9% Overall Service Availability within a billing month.**

Overall Service Availability is measured as a “Monthly Uptime Percentage” and is calculated via the following formula:

$$\frac{\text{Total available minutes per month} - \text{Downtime minutes}}{\text{Total available minutes per month}} \times 100$$

6.2 TOTAL AVAILABLE MINUTES PER MONTH

Total available minutes per month is the total minutes in the applicable billing month less Scheduled Maintenance.

6.3 DOWNTIME MINUTES

Downtime minutes is defined as the total minutes in a billing month in which the Service is unavailable, excluding (i) Scheduled Maintenance or (ii) unavailability of the Service due to issues described in the Service Level Exclusions below.

6.4 SCHEDULED MAINTENANCE

Scheduled maintenance events are planned, periodic updates, fixes or changes made by Service Operations to the Service environment. The majority of these maintenance tasks are performed without any impact on Service availability, but some maintenance tasks may require updates that make the Service unavailable for a short period. Service Operations will communicate any planned downtime to customers as per this Service Level Policy.

6.4.1 SCHEDULED MAINTENANCE NOTIFICATION

Notification Type	Target Notification Window	Notes
Notification of Scheduled Maintenance including minor Service updates not related to Service version upgrades	3 Days	Service Operations will provide three days' notice of Scheduled Maintenance. Notifications will be posted via the Service Status page.
Notification of Scheduled Maintenance for Service version upgrades	10 days	Customers will be notified in advance of planned Service version upgrades to allow for application testing against the new platform. Notifications will be sent to the primary customer contact for the Service.

6.5 UNSCHEDULED MAINTENANCE

Unscheduled maintenance events are considered unplanned, ad-hoc updates, fixes or changes made by Service Operations to address time-critical issues, and may result in unplanned downtime. Additionally, any outages of the underlying third-party datacenter which may affect the quality of the Service generally or a customer's Service environment specifically may result in unplanned downtime.

In case of emergency maintenance or downtime, Service staff will make reasonable efforts to communicate the downtime to affected customers.

6.5.1 UNSCHEDULED MAINTENANCE NOTIFICATION

Notification Type	Notes
Notification of unscheduled maintenance	For broader Service outages that require unscheduled maintenance, the Service Status

	page will be updated. Customers should subscribe to updates via the Service Status page. For isolated incidents within customer-specific tenants, Service staff will make all reasonable efforts to communicate the downtime directly to affected customers.

6.6 SERVICE LEVEL REMEDY POLICY

When Overall Service Availability of 99.9% is not met in a given subscription month, K2, after confirming the nature and accuracy of the availability issue, may credit the customer's account 10% of the monthly portion of the annual Subscription fee amount ("Service Credit") as provided below.

To receive a Service Credit, the customer must have opened a Technical Support Ticket for the availability issue, and the customer must notify the Customer Success Manager associated with the customer's Service within thirty (30) days of the end of the month in which the Overall Service Availability was not met to provide the following:

- The Technical Support Ticket number
- A detailed description of when the Service was not available including duration of the downtime
- How the customer was affected
- Description of the steps the customer initially took to attempt to resolve the issue

K2 reserves the right to withhold a Service Credit if it cannot verify the downtime or if the customer cannot provide evidence that they were adversely affected as a result of the downtime.

A customer must be in compliance with the Agreement in order to be eligible for a Service Credit. Customers in breach of the Subscription Agreement, including payment obligations, are not entitled to a Service Credit.

Verified Service Credits will be added to the customer's Service account balance for use upon subsequent renewal. No refunds or cash value will be provided.

6.7 SERVICE LEVEL EXCLUSIONS

Unless specified otherwise, the Overall Service Availability applies only to a customer's Service production environment. Service Credits for Overall Service Availability of non-Production environments are not offered.

Overall Service Availability does not include the following:

- A failure, degradation of performance or malfunction resulting from scripts, data, applications, infrastructure, software, penetration testing and/or performance testing directed, provided or performed by customer.

- Planned outages, scheduled maintenance, or outages initiated by Service Operations at the request or direction of customer for maintenance, activation of configurations, backups or other purposes that require the Service to be temporarily taken offline.
- Interruption or shut down of the Service due to circumstances reasonably believed by Service Operations to be a significant threat to the normal operation of the Service, the operating infrastructure, the facility from which the Service are provided, and/or access to, or the integrity of customer data (e.g., a hacker or malware attack).
- Outages due to unsupported system administration, commands or changes performed by customer users or representatives.
- Outages due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and other K2 vendors), and other force majeure events.
- Inability to access the Service or outages caused by the customer's conduct, including negligence or breach of the customer's material obligations under the Service, or by other circumstances outside of Service Operations' or K2 control.
- Lack of availability or untimely response time of the customer to respond to incidents that require customer participation for source identification and/or resolution.
- Outages caused by failures or fluctuations in electrical, connectivity, network or telecommunications equipment or lines due to customer conduct or circumstances outside of Service Operations' control.

6.8 NETWORK BANDWIDTH AND LATENCY

The Service is not responsible for a customer's network connections or for conditions or problems arising from, or related to, a customer's network connections (e.g., bandwidth issues, excessive latency, network outages), or caused by the Internet. This includes any connectivity between the Service environment and any resources managed by the customer. Service Operations monitors network performance within the Service environment, and will address any networking issues within the Service environment that may impact availability or latency.

7 TECHNICAL SUPPORT

Standard Technical Support is provided as part of the Service. Additional premium support is available for separate fees. The Technical Support Policy for the Service is available for review here: https://www.k2.com/legal/support-and-services-policies.

8 HIGH-LEVEL ARCHITECTURE

Figure 1 below illustrates the default high level architecture for the production environment of a K2 Nexus subscription.

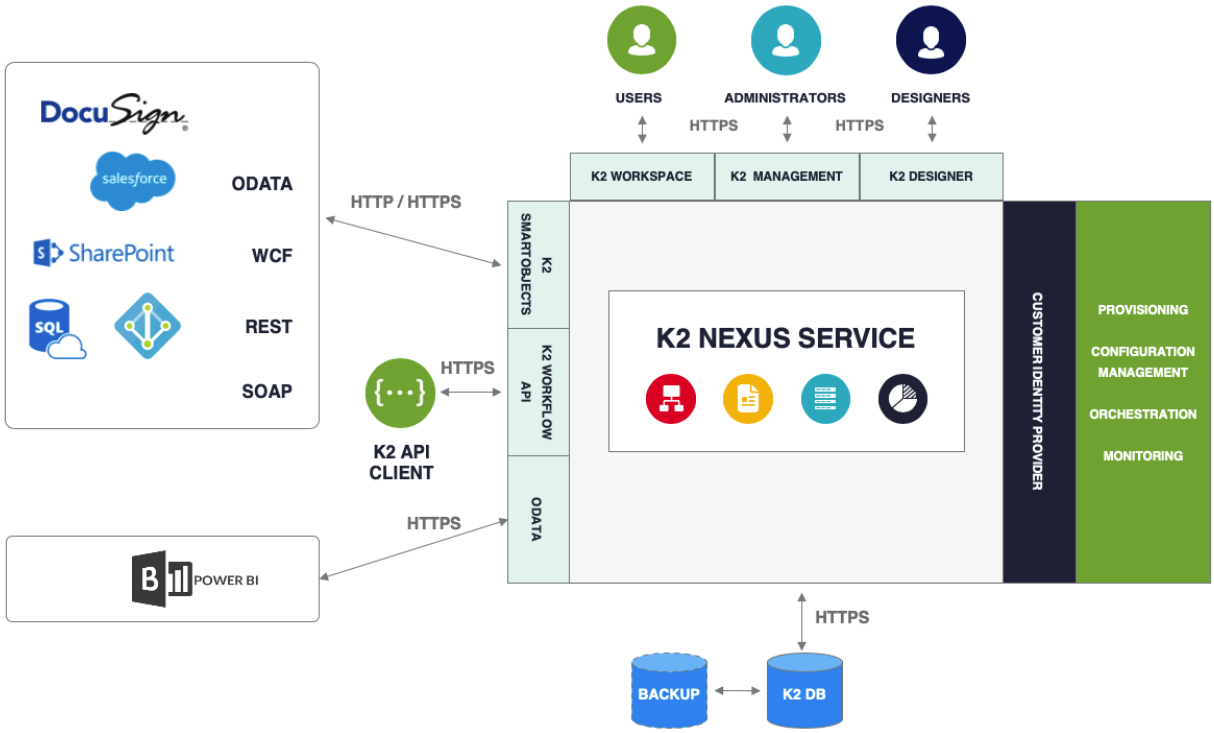

Figure 1 - K2 Nexus Architecture

9 DATA INTEGRATION

The Service natively provides the ability for customers to connect to data systems external to the Service as a means to integrate critical line-of-business systems into the applications that are being built utilizing K2 Nexus. These connections – called SmartObjects – can be configured either as a standalone read, standalone write or bi-directional read-write connections and allow for a customer to interact with data in the systems of record without importing data into and out of the Service for transient use within K2 Nexus applications. The data that is integrated via SmartObjects is not cached within the Service nor is it permanently stored in internal K2 Nexus data stores to ensure that customer data is always the most relevant version available.

9.1 STANDARD DATA INTEGRATION OPTIONS

K2 Nexus provides integration capabilities with the following external systems:

- Box
- Dropbox
- DocuSign
- Blue Prism
- Google Drive

- Microsoft Azure Active Directory
- Microsoft Azure SQL
- Microsoft Dynamics 365 Online
- Microsoft Dynamics 2013/2015/2016 *
- Microsoft Exchange Online
- Microsoft Exchange 2016/2019 *
- Microsoft OneDrive
- Microsoft SharePoint Online
- Microsoft SQL Server 2014/2016/2017 *
- Microsoft Teams
- Oracle 11g/12c *
- Salesforce
- SOAP/WCF/REST/OData web service endpoints
- UiPath
- K2 SmartBox

** could require this integration to be directly exposed to a K2 Nexus tenant or require the use of an additional connectivity service such as K2 Nexus VPN.*

Refer to Product Compatibility, Integration and Support for more details: https://help.k2.com/k2compatibilitysupportmatrix#intIntegration .

NOTE **Additional external data sources can be configured to connect to the K2 Nexus Service. Such connections may require additional configuration assistance which can be provided by K2 professional services.**

9.2 DATA INTEGRATION SECURITY

Each external system that can be integrated with the Service allows for definition of a Security Provider during configuration of the SmartObject. For all systems, the following Security Providers are available:

- Static
- Service Account
- OAuth

Customers should evaluate the authentication needs of the external systems that are being connected into prior to configuring data integration.

NOTE **Neither Service Operations nor Technical Support will provide assistance in configuring integration into specific external line-of-business systems. Documentation**

will be provided around specific integration-type capabilities via the K2 Learning platform. If a customer has specific requests not addressed by K2 Learning information, additional requests can be coordinated with the K2 professional services to provide specific one-on-one assistance.

10 SECURITY

Security of customer data and applications is of outmost importance to K2. Service subscriptions leverage the security features provided by the underlying infrastructure and system architecture. In addition, the Service constantly looks to improve security by applying new security features as they become available.

The Service has in place various procedural, administrative, technical, and physical safeguards to help protect subscriber accounts, K2 environments and data from loss, theft, misuse, abuse and unauthorized access, disclosure, alteration, and destruction.

10.1 ACCESS CONTROL

10.1.1 SYSTEM HARDENING

As part of the onboarding process and ongoing maintenance, the Service employs standardized system-hardening practices such as restricting access, removing or disabling unnecessary software and services, removing unnecessary user accounts, setting up network security, patch management, and logging.

10.1.2 SYSTEM AND APPLICATION ACCESS CONTROL, USER AND PASSWORD MANAGEMENT

Access to underlying Service environments by Services Operations is restricted to authorized personnel only. Service Operations' access to Service infrastructure is limited to remote connectivity only, secured with accounts controlled by Service Operations. The Service employs strong password policies, including restricted access to authorized usernames and passwords. Service Operations staff will be able to access and manage the K2 infrastructure with role-specific permissions, limited to the requirements of managing the Service.

In the event Technical Support needs access to a Service environment for troubleshooting, read-only database access may be granted to Technical Support for the explicit purpose of attempting to resolve an issue. Such access may include the ability to enable or disable logging and extract those logs for further review.

All access requests by either Service Operations or Technical Support will be logged for auditing purposes.

Customer resources will not be allowed to access the Service infrastructure. Administrative access to the Service by the customer will use the standard administration interfaces provided by K2 within the Service, and only when authorization is in place.

As the Service can integrate with third-party cloud applications and data (such as Salesforce, Azure SQL, private and public web services, etc.), integrating with these services may require additional, ad-hoc security and communication configuration based on the technology being integrated and the specific use case of the integration.

The customer is responsible for all end user and application administration within the Service environment. K2 does not own, control or manage the customer's end user accounts or applications in the Service environment. Customers may configure the environment and applications on the Service environment using K2's built-in security features, authorization protocols and administration tools. Customers are responsible for managing and reviewing access for their own employee accounts.

For details on specific authorization for Service environments, please refer to the Authorization section of these policies.

10.2 INFRASTRUCTURE SECURITY

All physical Service infrastructure is hosted on reliable and scalable global datacenter infrastructure with very strict physical access security policies. In addition to infrastructure-specific security policies, the Service subscription adheres to additional industry recognized security and certification policies such as ISO 27001 2013 and other standards. More details on security certifications of the K2 Nexus Service are available in the Security Certificates and Details section.

Neither K2 nor any customer resources will have physical access to the machines or infrastructure in any Service environment. Only members of the Datacenter Operations staff are granted physical access to underlying machines or infrastructure within the Service environment.

10.3 AUTHENTICATION

A Service environment will leverage one of the following provider types:

- Microsoft Azure AD – integration provided via Azure AD apps specified for the use of integration with the Service and a customer's Azure AD environment. If a customer has enabled Multi-Factor Authentication within their Azure AD infrastructure, this will also be included within the authentication pipeline for any users within the Service as well.
- OpenID Connect and SCIM providers – integration with identity providers that have valid OpenID Connect and SCIM 2.0 capabilities which allow for the customer to push identities into the Service.

The Service does permit SmartForm Anonymous Access if desired. This access is configured and enabled as per the standard Anonymous Access configuration supported by K2 SmartForms.

NOTE **In certain cases, non-AAD credentials could be used to integrate with systems, such as when Basic, Static or OAuth Authentication Modes are used by SmartObjects to integrate with external systems. Such integration is the responsibility of the customer and not provided as a feature of the overall Service.**

10.4 AUTHORIZATION

Authorization policies are applied to ensure that appropriate rights and permissions are in place to restrict access to Service resources and allow only the access that is required to achieve specific tasks. It is possible that certain application requirements may require additional permissions, or that ad-hoc authorization may be required to address issues in the environment. K2 will not make any authorization changes without prior notification, and subject to documented agreement by the customer.

The tables below describe the base-level authorizations that are applied in Service.

10.4.1 SYSTEM ACCESS AND APPLICATION AUTHORIZATION

Virtual access to machines and access to supporting applications will be restricted to minimum permissions that will allow the infrastructure and applications to operate. The table below describes some machine and software authorization that apply in a Service implementation

Securable Component	**Permissions**	**Roles**	**Notes**
Service underlying infrastructure and components	Access through Service administration interfaces	Service Operations Technical Support	Service Operations staff will have remote access to the Service environment and be able to perform administrative operations to the infrastructure. Technical Support may be allowed read-only database access to the customer environment for the express purpose of attempting to resolve a customer issue. Technical Support may enable/disable logging and export logs for review. All access requests by Service Operations or Technical Support are logged for auditing purposes.

			Customer users will not be allowed to access the Service infrastructure.
Customer's Microsoft Azure subscription and Microsoft Azure Services	Access through Microsoft Azure administration interfaces	Service Operations	For customers utilizing the native Azure AD integration, Service Operations will not have any access to the customer's Microsoft Azure environment through any of the Microsoft Azure administration interfaces.
	Microsoft Azure Active Directory API access	K2 Nexus	For customers utilizing the native Azure AD integration, the Service utilizes a service account to allow the Service to integrate with the customer's Microsoft Azure AD (AAD) store and utilize these AAD identities for authentication within the Service. Consent for the Service to access a customer's Microsoft Azure AD tenant will be granted by the customer's Microsoft Azure AD Tenant Administrator during the Service onboarding.
Identity provider services	Identity provider access	K2 Nexus	The Service can utilize SCIM to push identities from the customer's identity provider into the Service; however, via this setup the Service does not have the ability to pull identities into the Service.
Customer servers	Administrative access	Service Operations	For customers that have established a direct connection between the Service and on-premises systems, Service Operations staff will not have access to customer servers or

			machines in the customer environment.
K2 database	Database administration and ownership	Service Operations Technical Support K2 Service Account	Service Operations will have administrative access to the K2 databases. Technical Support will have read-only access to the K2 databases. The K2 Service Account has the ability to interact with the K2 database as well.

10.4.2 INTEGRATION-SPECIFIC AUTHORIZATION

Integration with applications outside of the Service environment (such as interacting with cloud-based data providers or on-premises data sources) will be application-specific and subject to the particular requirements of the application. For example, some integration may leverage OAuth token flow. The target system can then apply authorization based on the credential used by K2 for integration. In all cases, the specific authentication mode and authorization applied will be established based on the application requirements and the infrastructure support. As such, it is not possible to provide integration-specific authorization information because the authorization necessary will depend on the integration.

10.5 NETWORK TRAFFIC SECURITY

Customers will connect to the Service via the following different primary mechanisms:

- Directly to Service tooling via a web browser
- By utilizing third party reporting tools
- Via customer-managed, custom applications
- Via a device-specific K2 Mobile application

In each of these scenarios, traffic between the Service and the customer will travel over secure and encrypted TLS/SSL channels.

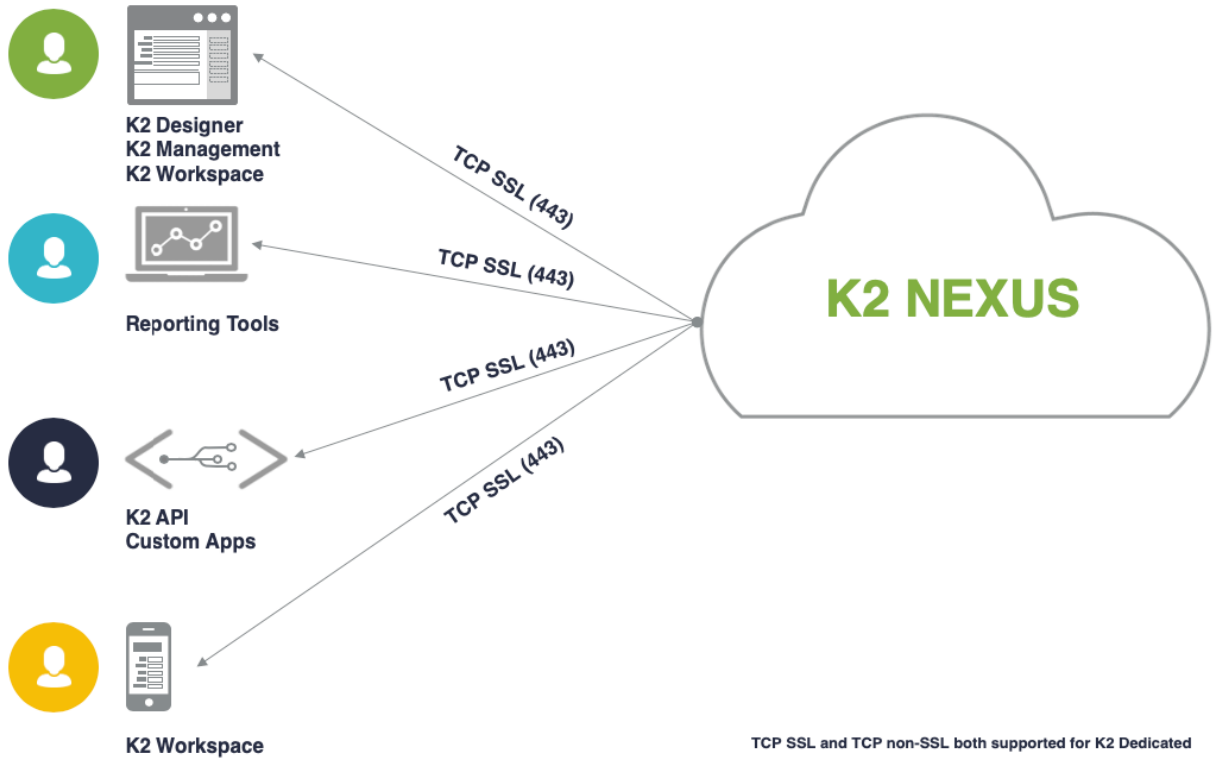

Figure 2 - Network Security of connections to K2 Nexus

10.5.1 DATA TRANSPORT ENCRYPTION

As data is either retrieved or generated from within the Service, it is secured during transport to the client. Internal network traffic within the Service environment is secured using network subnets utilizing Access Control Lists (ACLs) to restrict network communication to resources within the Service environment only. All communication is made over secure and encrypted channels.

For customers that are connecting to systems external to the Service via SmartObjects, secured communication channels should be utilized whenever possible.

10.5.2 NETWORK AND FIREWALLS

All data communication within the Service environment (for example, communication between the K2 application servers and the K2 database) occurs within the underlying protected network and does not touch the public Internet until data is returned to the calling client via secured TLS/SSL channels.

10.5.3 ISOLATION AND SEGREGATION

Each Service subscription, along with the resources within that subscription (including the K2 environments, servers, data storage and network communication), is logically separated per customer.

10.6 DATA SECURITY

Data stored within the Service are kept separate in individual customer environments and is isolated from neighboring environments.

The data stored in the Service itself is protected from unauthorized access with underlying data infrastructure security applied to logins and roles, based on the standard minimum-permission model applied by the Service. Any data that is stored by a customer as the result of building applications on the Service is encrypted at rest within the Service via Transparent Data Encryption (TDE); more details about TDE are available here: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption.

10.6.1 TRANSIENT DATA

The Service architecture is designed to securely retrieve or update data in real time from external systems. When communicating directly with an external system, SSL configuration is recommended for every connection between the Service and an external system; however, this is ultimately at the discretion of the customer when establishing connections. See Network Traffic Security section for additional details.

Although data flows directly from the external system through the Service to the client and is never permanently stored, the Service does make use of Microsoft SQL Server Common Table Expressions (CTEs) for internal operations such as SmartObject disparate data joins and normalization. A CTE is similar to a derived table in that it is not stored as an object and lasts only for the duration of the query.

NOTE **Customers should be aware that the database roles required for maintaining a K2 database means that Service Operations may have access to the data stored in the K2 SmartBox data stores. Service Operations is restricted from altering, deleting or extracting that data from the Service.**

Any interaction that Service Operations has with customer data stored within the Service is only initiated after a customer logs a Technical Support ticket to address a particular issue, and never without direct customer request and notification.

10.6.2 BACKUP DATA

Customer application data, system configuration data and underlying Service database and database backups are securely stored as part of the Service High Availability capabilities.

10.6.3 CUSTOMER DATA OWNERSHIP

K2 does not claim ownership of customer data in the K2 database. To obtain such stored data from the Service, a customer must initiate a request via the Technical Support ticket system indicating they would like to obtain such data. Technical Support will work with Service Operations to provide an extract of the data in a timely manner. More details are available in the Customer Data Ownership Rights section.

10.7 MOBILE DEVICE SECURITY

Communication between devices operating the K2 Mobile App and the Service environment will occur via the HTTPS-secured connection to the public-facing K2 web-service endpoints and websites.

Data for the K2 Mobile App is stored in a device-specific local database on the device and locally encrypted. Additionally, user credentials are encrypted using device-specific encryption capabilities. For specific details on K2 Mobile App Security, please refer to the K2 Workspace App Security page on help.k2.com.

10.8 SECURITY INCIDENT RESPONSE

While reasonable precautions are taken to secure Service environments from security threats and breaches, in any connected environment there is always a risk of security incidents that might originate from external or internal threats. The Service has in place certain teams, policies and procedures to deal with security incidents.

Security incidents that are not automatically detected by Service Operations can be reported through the normal support channels, or in case of emergency, contact security@k2.com.

10.8.1 COMPUTER SECURITY INCIDENT MANAGEMENT TEAM (CSIMT)

K2 has established a Computer Security Incident Management Team (CSMIT) to resolve Service security incidents. The table below describes the roles and responsibilities of the CSIMT:

Role	Responsibility
Technical Support Engineer	The Technical Support Engineer is the first line of support when reporting any security incidents and will initiate CSIMT responses.
Service Operations Manager	The Operations Manager will begin to isolate the incident and preserve any forensic evidence.
Service Chief Engineer	The Chief Engineer will work with the Operations Manager to determine the scope of the incident.

Service Security Analyst	Security Analysts will assist the Chief Engineer to better understand the nature and root cause incident.
Service Engineering Director	The Engineering Director owns the CSIMT process and works with all other team members to ensure the proper steps are followed and the incident is addressed and documented with appropriate action towards resolution.
Security Officer	The Security Officer will coordinate with executive leadership for risk and damage analysis and consolidate all communications to inform subscribers and media of any incidents.
General Counsel (GC)	This role is primarily responsible for overseeing legal and liability matters, including liaising with local, state and federal authorities.

10.8.2 INCIDENT RESPONSE PLAN

In the unlikely event of a security-related incident or breach, K2 has a system to report, contain, analyze, communicate and resolve security related incidents. This incident response plan outlines the roles and procedures in place for responding to security incidents involving the Service, infrastructure and systems. The plan does not cover security breaches within a customer's internal environment or other third-party environments connected or integrated into the Service.

1. Monitoring
    a. Service Operations actively monitors automated metrics for system level events and will investigate and report incidents accordingly.
    b. Service penetration tests are performed periodically and identified issues are addressed.
    c. Customers are encouraged to monitor for any unusual activity or behavior and report any suspicious or malicious events immediately by contacting Technical Support.

2. Incident Reporting and Escalation
    a. All security related incidents must be reported to Technical Support Engineers who will log the incident and begin primary investigation.
    b. If the primary investigation warrants escalation, the Technical Support Engineer will escalate to the Service Operations Manager, Service Chief Engineer and Service Engineering Director.
    c. Following investigation, if the incident is a valid security incident, the Security Office is notified and assists in the incident response.

3. Containment
    a. The Technical Support Engineer, Service Operations Manager and Service Chief Engineer will initiate an immediate lock-down procedure to contain the incident and preserve any forensic evidence.

b. The Service Engineering Director will oversee the containment process and notify the Security Officer of the incident.
c. The Security Officer will notify subscribers of any planned downtime due to lockdown and containment procedures.
d. if additional help is required, outside forensic assistance may be utilized to assist in the investigation.

4. Analysis
    a. The Service Engineering Director will coordinate with all involved parties to analyze the extent of the incident.
    b. The Security Officer will coordinate with executive leadership to analyze the financial and material impact of the incident.
    c. The Engineering Director and the Security Officer will work together to determine the scope of the incident and how Service business continuity may be affected.

5. Communication
    a. The Security Officer will work with the General Counsel to involve outside authorities if required.
    b. The Security Officer will coordinate timely communication with customers regarding the incident and expected business continuity disruption.

6. Resolution
    a. The Engineering Director will determine next steps to resolution and if any Service change requests are needed.

10.9 SECURITY CERTIFICATES AND DETAILS

K2 understands how critical it is for customer applications and data to be secure no matter where they run. We utilize a rigorous program of third-party audits to ensure cloud security and compliance across a number of industry standards.

10.9.1 ISO 27001:2013

ISO 27001:2013 is a widely accepted set of international standards relating to the secure management of information, particularly in a cloud-based environment. The Service has been independently verified to meet all ISO 27001:2013 standards for cloud security and information management. More details about ISO 27001:2013 are available here.

10.9.2 SOC 2 TYPE 2

The American Institute of Certified Public Accountants (AICPA) developed the Service Organization Control (SOC) framework which outlines controls that organizations can implement and be assessed by to protect the confidentiality and security of information in the cloud. Our SOC 2 Type 2 report evaluates controls that are relevant to security, availability, and confidentiality over a defined period of time. The Service is independently audited by a third party that verifies compliance of SOC 2 controls. A copy of our latest SOC2 Type 2 report can be obtained by request, with a signed NDA.

10.9.3 SOC 3

The SOC 3 Report, just like SOC 2, is based upon the Trust Service Principles and performed under AT101, the difference being that a SOC 3 Report can be freely distributed (general use) and only reports on if the entity has achieved the Trust Services criteria or not (no description of tests and results or opinion on the description of the system). SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality and privacy) and allow the organization to place a seal on its website upon successful completion.

11 INCIDENT RESPONSE

The following section details disaster recovery capabilities of the K2 Service.

11.1 DEFINITIONS

11.1.1 INCIDENT

An incident refers to any single event or any set of events that result in downtime.

11.1.2 DISASTER

For the purposes of this policy, a disaster is defined as an unplanned event or condition that causes a complete loss of access to the customer's production Service instance.

11.1.3 RECOVERY POINT OBJECTIVE (RPO)

RPO is commonly defined as the amount of time between a data backup and when the disruptive event occurred.

11.1.4 RECOVERY TIME OBJECTIVE (RTO)

RTO is the maximum loss of availability following a disruptive event measured by the maximum amount of time before the application fully recovers.

Figure 3 - Visual representation of RPO and RTO

11.2 HIGH AVAILABILITY AND REDUNDANT INFRASTRUCTURE

A Service environment is built on redundant and resilient infrastructure, designed to maintain high levels of availability and provides the ability to recover the Service in the event of a significant disaster or disruption.

Production environments feature high availability architectures to ensure that failure of a single node will not affect production availability. These same capabilities are optionally available for non-production environments for separate fees.

11.2.1 NETWORK

Network infrastructure is duplicated where possible (e.g., duplicate NICs) as per the third-party datacenter provider's policies, or otherwise virtualized for rapid replacement.

11.2.2 APPLICATION SERVERS

Application servers are load-balanced and redundant, so that a failure of all but one application server will not result in system downtime.

11.2.3 DATABASE SERVERS

Database storage is continuously backed-up and can be restored to a point-in-time.

11.3 DISASTER RECOVERY AND DATA RESTORATION STRATEGY

The Service maintains internal business continuity plan (BCP) and disaster recovery (DR) policies in support of certifications such as ISO27001:2013.

A Service subscription includes disaster recovery (DR) for the production environment which is intended to provide Service restoration in the event of a major disaster, as declared by the Service.

Data restoration is available in the event of a DR event or upon customer request.

NOTE **The disaster recovery datacenter may not be geographically close to a customer site and may incur different latency responses from the Service.**

11.3.2 SERVICE LEVEL – FAILOVER AND DISASTER RECOVERY

Item	Target Response Objective	Notes
Recovery Time Objective (RTO)	Within 48 hours after DR event	This refers to the time necessary to restore the Service following a disruption event.

11.3.3 DATA BACKUP AND RESTORE STRATEGY

Data pertaining to the customer's configuration of the Service resides solely in the K2 database and is natively backed-up.

Should a database restore be required (either due to a DR event or following customer-initiated request for restoration), the restore operation can be initiated by submitting a Technical Support request. Details about the impact of a database restore within a customer's tenant can be discussed with the Customer Success Manager and/or Technical Support Engineer as needed.

11.3.4 SERVICE LEVEL – DATA BACKUP

Item	Target Response Objective	Notes
Recovery Point Objective (RPO):	1 hour or less	K2 database which contains K2 configuration data as well as any data stored by the customer in K2 SmartBox SmartObjects can be restored to any restore point within 14 days. Restoration of data is also subject to the Database RTO Service Level detailed above.
Data backup retention period	14 days of backup data	Retention of last 14 days of the underlying K2 database backups. K2 database restores can revert backups to any restore point within 14 days. Restoration of data is subject to the Database RTO and RPO Service Levels.

11.4 MEASUREMENT AND MONITORING

The Service includes automatic measurement and monitoring of the underlying infrastructure and network communication for the Service environment. Any monitoring outside of the Service infrastructure (such as network connectivity to the customer site, or availability of customer systems that integrate with the Service) is not included in the Service. Measurement and monitoring of application-specific performance metrics is not included.

Service Operations monitors system availability constantly and will communicate any availability issues as soon as possible. System status, availability, performance and security notifications and issues will be posted via a Service status webpage.

In addition to the general status updates posted to the Service status site, Service Operations internally monitors various environmental performance, usage and stability metrics. While these metrics are not shared with customers, they do provide monitoring and fault identification capabilities to Service Operations and are a key tool utilized to make sure that a customer's environment is stable, available and performing to standards.

12 CHANGE MANAGEMENT

Change control policies are in place to ensure that only approved and audited changes are applied to the Service environment. There are two main categories of change management, each with specific policies that are described further in this section.

12.1 SERVICE-INITIATED CHANGES

Service-initiated changes include those applied during scheduled or unscheduled maintenance and will be communicated as per the defined Service Level. For changes that will not affect Service availability or application stability, Service Operations will apply such changes without notice, but in all cases, will retain history of changes applied for auditing purposes.

12.2.1 K2 SOFTWARE UPDATES

Service environments are subject to standard product updates provided by K2. As such, any software updates to the Service. For more information on K2 releases, please refer to K2 Product Release Strategy.

12.2.2 STAGGERING K2 SOFTWARE UPDATES

Customers have the ability to request a delay in scheduled service-initiated changes of a production environment to allow for testing in associated non-production environments prior to the update of their corresponding production environment by coordinating with their Customer Success Manager. A production environment service-initiated change can be delayed by a maximum of five business days.

For customers that have both a production and development environment, both environments must be updated to the same version within a given Service update period.

NOTE **It is important to note that the migration of solutions between non-production and production environments via the K2 Package and Deployment (P&D) tool will not be possible during the duration of this delay.**

A production K2 Nexus environment can only be delayed further in cases where an issue is discovered during regression testing of a customer non-production environment that would introduce the same issue within production.

NOTE **There are certain circumstances in which delaying the upgrade of an environment cannot be scheduled – specifically when multiple environments share either a Microsoft Azure Active Directory tenant and/or a Microsoft SharePoint Online tenant. A change to either of the K2 apps associated with these types of tenants will render other connected tenants potentially problematic; all tenants that share resources such as these should be upgraded at the same time.**

12.3 CUSTOMER-INITIATED CHANGES

Customer-initiated changes may include:

- Packaging applications from within a non-production environment
- Deploying applications into a production environment
- Configuring the Service

The Service will not allow customers to make changes to the standard Service environment through custom code or other unique customizations that would alter the standard functions of the Service.

The non-production environment within the Service duplicates the production environment so that testing of applications in the non-prod environment is representative of the production environment (outside of applications developed and deployed within the production environment) and to facilitate easy migration between non-production and production environments.

13 ACCEPTABLE USE POLICY

Use of the Service is conditioned on this Acceptable Use policy. A customer shall not:

- Allow anyone other than authorized users to use the Service
- Sell, resell, license, sublicense, rent, lease or share the Service, or use the Service as an application service or outsourcing offering
- Use the Service to store or send any infringing, libelous or otherwise tortious or unlawful data or material, or any data or material in violation of third-party privacy rights, or to send junk mail or spam
- Use the Service to store or send any computer viruses, time bombs, worms, Trojan horse code, and/or other malicious or harmful code, macros, scripts, files, programs or agents
- Attempt to gain unauthorized access to the Service or applicable infrastructure
- Interfere with or disrupt the delivery of the Service or any data or other material utilized or stored by the Service
- Cause or permit the reverse engineering, de-compilation or disassembly of the Service or any portion thereof, except and only to the extent that such activity is expressly permitted by applicable law
- Disclose results of any Service benchmark tests without K2's prior written consent
- Use the Service for purposes of competitive analysis or development of a competitive offering

14 SUSPENSION AND TERMINATION POLICY

14.1 TERMINATION OF SERVICE

For 35 days after the termination or expiration of the Service, K2 will keep available customer production data – if any – for retrieval by the customer. After such 35 days, K2 will have no obligation to retain the customer data, and K2 shall delete any customer data from the Service. A customer can request immediate deletion of any customer data from Service upon termination as well. Upon request, K2 will issue the customer with a certificate validating the deletion of data.

Within the 35-day post-termination period, a customer may request production environment data retrieval through Technical Support. K2 will provide assistance to allow the customer to retrieve or export such data from the customer's production Service K2 database. Data will not be made recoverable for customer non-production environments.

14.1.1 TERMINATION OF TRIAL ENVIRONMENTS

K2 will not retain data used in any trial or proof-of-concept environments after the applicable evaluation period has expired.

14.2 SUSPENSION OF SERVICE

K2 may temporarily suspend customer access to or use of the Service if the customer or users acting on behalf of the customer violate any provision of the Subscription Agreement or these policies, or if in K2's reasonable judgment, the Service or any component thereof are about to suffer a significant threat to security or functionality. Service Operations will make reasonable efforts to provide advance notice to customers of any such suspension and to promptly re-establish the affected Service once the issue has been remedied.

14.3 CUSTOMER DATA OWNERSHIP RIGHTS

Each customer retains ownership of its data residing in the Service database. K2 has no ownership rights in such customer data.