KURTOSYS

Pain-free investment data
and insight delivery

Standard Support Promise

NOVEMBER 2022

Service Level Agreements ("SLA")

1. **Introduction**

    At Kurtosys we strive to provide the highest level of customer support that reflects our commitment to being your trusted partner. The purpose of this Support Promise is to provide you with an explanation of how our support service operates. This support promise is a part of your agreement with Kurtosys and subject to the definitions and provisions in the terms of use.

2. **Definition of terms**

    a. **Support Hours** are the times agreed for response and services provided. **Standard Support Hours** are based on business hours in which the Support Desk and Support Staff are online. For other, **Out of Hours Support**, a monitoring service operated with "on call" responders.
    b. **Incident** is a failure of the service provided by Kurtosys related to issues of Confidentiality, Integrity and Availability.
    c. **Support Ticket** is the mechanism by which an **Incident** is raised by the client with Kurtosys and which provides a record of communication between the two Parties to manage the resolution of the **Incident**. These communications will include updates that inform both parties of remediation plans and probable causes up and to the point of remediation.
    d. **Priority Status** is the designated status of the **Incident** and defines the severity and type of the incident which dictates the form of response and escalation.
    e. **Classification Labels** are attributes of the **Incident** which are added to characterise the nature of the events and actions required. These may be added and updated throughout the duration of the **Incident**.
    f. **Remediation** is the process of correcting the effects of the **Incident**.
    g. **Incident Report** is the final report provided to the Client by Kurtosys which documents:
    *   the details of the Incident
    *   resolution steps taken to remediate the Incident
    *   subsequent investigation and analysis of the incident to establish a Root Cause ("**RCA**"), and
    *   conclusions and further actions recommended to resolve Root Cause issues with the purpose of preventing recurrence
    h. **Acknowledgement** is the initial notification added to a **Support Ticket** confirming receipt of a reported **Incident**
    i. **Updates** are notifications added to **Support Tickets** according to a specified frequency up until remediation takes place. These will include details of proposed remediation plans and probable causes up and to the point of remediation. They are not intended to summarise a full analysis provided in the **Incident Report**

3. **Support Process**

    a. **Standard Support Hours**

        We provide standard service desk support between 08:00 GMT (08:00 UTC) and 17:00 US PST (01:00 UTC), Monday to Friday, excluding Regional (US, UK, South Africa) Bank & Public Holidays, where hours of operation will be shortened based on the business offices that remain open.

        If you have a support query or discover an incident, please contact our support team by logging a ticket via the service desk customer portal or by sending an email to support@kurtosys.com

Ideally, your ticket or email should provide the following information:

i. Date & time of incident
ii. Contact name(s) for follow-up
iii. Your incident classification (critical (P1), major (P2), minor (P3) – defined below)
iv. A description of incident
v. A description of impact to service
vi. The user details/URL used to access the product and service when the incident occurred
vii. Steps on how to reproduce the incident
viii. Screenshots/other information you feel would be helpful to us in resolving the incident

The more information is provided with the ticket, the faster we can work on a resolution. With all logged tickets (Incidents, Service Request and Change Requests) the Kurtosys support team follow a 3 day process on ticket administration for tickets in "Awaiting Customer Feedback" status. Tickets which receive no feedback from the customer for 3 consecutive days, will prompt an automatic closure on the service desk.

b. Out of Hours Support

Our internal systems automatically monitor our services and underlying servers. For all out of hours support, clients should continue to raise tickets as described above and these will be processed immediately at the start of the following day, except for critical P1 Incidents as described below.

i. Kurtosys uses monitoring technology to evaluate availability.
ii. Critical platform outages will automatically be escalated internally.
iii. Out of hours tickets from you are captured via service desk ticket logging, the issue will be logged and responded to on the next business day, unless the incident is a critical (P1) platform incident, in which case the support team are notified for a P1 response.
iv. An on call rota system operates for critical and emergency notifications.

4. Incidents

a. Incident Management

The Incident Management Process is defined in our ISO 27001 framework.

i. All incidents will be prioritised and actioned according to the service levels provided below.
ii. Any interruptions and reduction in service or quality of service related to incidents will be measured and reported.
iii. Any incident that involves a security breach will result in immediate notification and follow our security Incident Response Plan.
iv. All incidents will be investigated, and remediation plans presented by relevant teams responsible for remediation and communicated through support tickets or other channels according to escalation processes.
v. The incident report will contain a root cause analysis and details of remediation.
vi. If a root cause is identified, it may be shared earlier in notifications by email/phone. For other types of errors, a root cause can be supplied if requested.
vii. Application errors, errors due to erroneous data in files, and unanticipated interactions of configuration are not classified as platform incidents, and an explanation of the error will be emailed.

b. Priority and Service Levels

P1 Status

Definition	The entire platform/service is down and unavailable. The problem results in regulatory or financial liability due to operational or informational deficiency. A security breach has occurred resulting in loss of data or control of the application.
Support Ticket acknowledgement	< 1 hour
Support Ticket updates frequency	Approx. 30 mins
Remediation	< 4 hours from acknowledgement
Incident Report	5 business days from remediation

P2 Status

Definition	The platform/service is available but with issues that have a direct impact on productivity and performance of day-to-day activities.
Support Ticket acknowledgement	< 2 hour
Support Ticket updates frequency	Approx. 60 mins
Remediation	< 8 hours from acknowledgement
Incident Report	5 business days from remediation

P3 Status

Definition	The platform/service is available and core business is unaffected, but with intermittent or minor issues affecting efficient operation and / or creating a poor user experience.
Support Ticket acknowledgement	< 2 hour
Support Ticket updates frequency	Approx. 60 mins
Remediation	< 8 hours from acknowledgement
Incident Report	5 business days from remediation

c. Incident Classification

In addition to the Priority Status, Classification Labels will be applied to characterise the incident, and these may serve to modify the initial Priority Status, escalate or deescalate actions according to the investigation and analysis of the events.

i.   When an incident occurs, please first undertake an internal investigation to determine whether the cause is internal, due to a third party, or due to Kurtosys.
ii. If you believe the incident originates with Kurtosys, please log a ticket using the service desk customer portal or send an email to support@kurtosys.com, or if a critical P1 incident occurs

outside of support hours phone us, following the process outlined in the "Support" section above.

iii. We acknowledge that classifying an incident is not always clear cut, but we appreciate you applying the incident classifications as accurately as possible. This enables us to properly and fairly escalate our responses and to provide a better service to all our customers.

iv. In the rare event we don't agree with your incident classification, we will communicate and agree to an alternative classification.

d. Service Level Credits

Service Level Credits will be issued in accordance with agreed formula in our Client Contracts and subject to:

- Different incident types
- Duration of Outages
- Frequency of Incidents
- Incident remediation and reporting
- etc

5. Platform

a. Platform Availability

You will be able to access the Products and Services to which you subscribed as per the Order Form 99.8% of the time, twenty-four (24) hours a day, seven (7) days a week. Availability is evaluated quarterly.

i. This excludes any regular planned downtime which will be scheduled during non-business hours which are between 01:00 and 06:00 GMT weekdays and between 01:00 GMT Saturday and 23:00 GMT Sunday weekends.

ii. Regular planned downtime is one (1) hour or less, and we will provide a minimum of seven (7) days' notice. In most cases, we will declare a window, but do not expect there to be any downtime.

iii. No more than four (4) times per year, we will schedule major planned downtime which may last up to six (6) hours per datacentre, and we will provide a minimum of four (4) weeks' notice.

iv. Any unavailability caused by or arising from circumstances beyond our reasonable control is also excluded from availability calculations. This includes any infrastructure or other failures, delays, or unavailability caused by or contributed to by you or a telecommunications service provider, internet service provider, or any other provider of a non-Kurtosys application that is not a service provider directly to Kurtosys, or an act of force majeure.

b. Platform System Monitoring

All our systems are electronically monitored 24/7, 365 days a year.

i. Our services (applications, databases, servers, network, etc.) are monitored.

ii. All alerts are logged and distributed by our monitoring and alert systems.

iii. Multiple levels of monitoring consist of: Data Monitoring, Infrastructure Monitoring and User Interface Monitoring.

iv. Our technology and support teams are automatically notified of an event or incident via our regular communication channels.

c. Service Requests

A request for information or advice, or for a standard change (a pre-approved change that is low risk, relatively common and follows an agreed procedure). An example of a service request is a password reset.

Service Requests are not subject to measurement against service level metrics.

d. Changes

An alteration to an existing product or system functionality. More specifically the requested change is not part of the current functionality or provided service. A change request often arises when the customer wants an addition or alteration to the agreed-upon deliverables.

Changes are not subject to measurement against service level metrics.
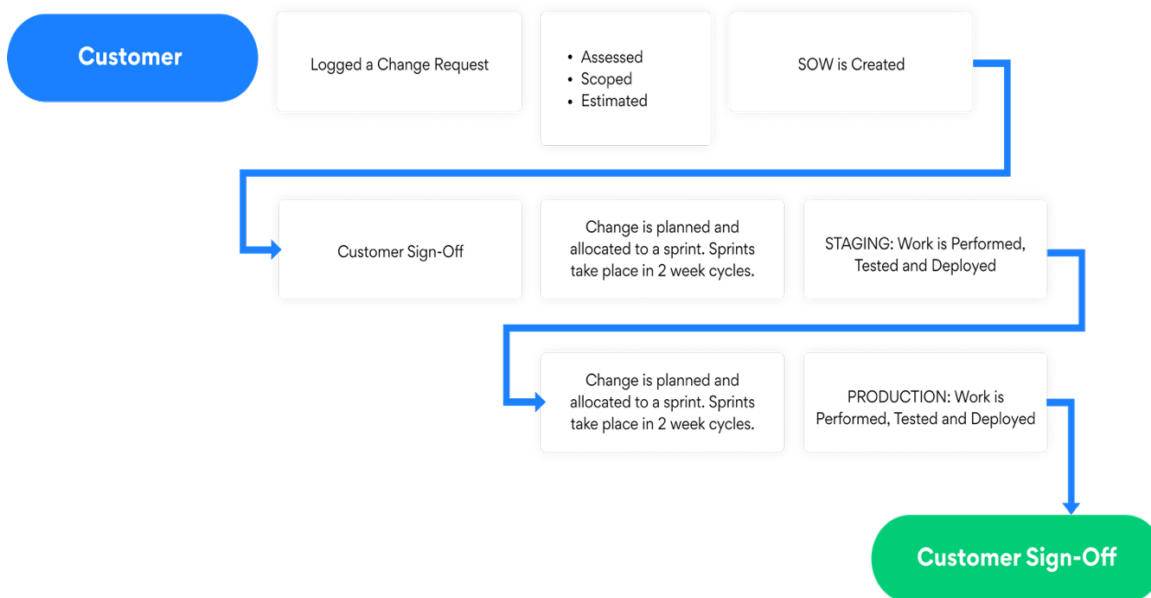
e. Change Request Process

Figure 1: Process Diagram: High-level change request process

f. Platform Change Management

All changes are subject to a change management process as defined by our ISO 27001 program.

i. Our Change Control system is based on a Jira service desk workflow; all changes are reviewed and tracked for reporting purposes and approvals granted by persons with relevant responsibility.
ii. The Change Control approval ensures changes are documented, tested, resourced, and a rollback plan is in place.
iii. The Change Control system approval is a dynamic process and includes escalation for emergency changes.

6. Reporting

a. Quarterly Reporting

Quarterly reporting of availability and incidents are provided by your Customer Success Manager on request. These will include:

i.   All incidents impacting availability are reported.
ii. A summary of support cases would including ticket classification level and type.
iii. We will also provide platform availability reports at an agreed frequency.

b. Incident Reporting

All incident reports will be delivered within 5 working days unless notified and subject to extended investigation. Any incident tickets will provide status notifications at the agreed intervals up to remediation.

7. Security

We will ensure that your data and the services that deliver your data to end users are protected and managed by applying suitable controls to maintain appropriate confidentiality, integrity and availability associated with our services.

i.   We have implemented ISO 27001 which is certified by an external auditor annually. This includes an ISMS and implements all of the security controls with the exception of payment cards. This determines how we operate, as well as how we classify and handle data.
ii. We use Cloud based IaaS (Infrastructure as a Service) provided by Amazon Web Services, a certified vendor, in resilient and secure datacentres within appropriate data jurisdictions.
iii. Our infrastructure is monitored, maintained, and protected by antivirus and anti-malware software, including checks of incoming files. Data is encrypted at rest and in transit.
iv. We apply WAF (Web Application Firewall), DDoS (Dynamic Denial of Service) and other IDS/IPS protection to all network traffic.
v.   We have Risk Assessment and Vulnerability Management programs to confirm our security controls are effective.

If you have a security issue that you wish to report or make an enquiry about, please email these to informationsecurity@kurtosys.com

8. Business Continuity and Disaster Recovery

We will ensure that your service is synchronised across datacentres in the same region and data is backed up so that we can restore your services in the case of a DR event. This defined by our ISO 27001 Business Continuity Policies.

i.   Databases are backed up frequently during the day consistent with the recovery point objective (RPO - https://en.wikipedia.org/wiki/recovery_point_objective) of one (1) hour in the appropriate secure cloud environment. Snapshots of the application servers are taken with backups.
ii. Backups are stored daily for one (1) week and are then available for one (1) month.
iii. Standard DR is based on failover between active:active datacentres and/or a rebuild of the last backup.
iv. Recovery time objective (RTO - https://en.wikipedia.org/wiki/recovery_time_objective) is four (4) hours.

9. Capacity Management

We will ensure that there is enough compute, storage and network resources to deliver our products and services.

i. Capacity management is handled at the platform level and includes automated load balancing across datacentre.
ii. Our platform is horizontally and vertically scalable to maximise operational availability with no single points of failure.
iii. Data loading is monitored to ensure operational integrity.
iv. Our Cloud Infrastructure providers have Service Level Agreements and certifications for provisioning and service delivery.

10. Out of Scope

All other support services are out of scope.

i. We would be happy to review additional support services, including our Managed Service/Premium Support offering which provides additional premium services as part of our overall customer care package.
ii. In exceptional cases we may be able to provide customized care services, however, any such services may require additional one-time implementation and on-going service fees.

This support promise document is issued on 1 November 2022 and is subject to periodic updates which will be made available through our web site at www.kurtosys.com.

KURTOSYS

Kurtosys provides a range of technology solutions to asset managers, creating efficiency within their distribution teams, empowering marketers, and facilitating stronger relationships with investors. Through our unique, cloud-based platform we provide all the tools required to build engaging investor websites and portals, automate sales collateral, and distribute critical reporting to clients.

The Kurtosys platform replaces many of the traditional point-solutions used across sales and marketing, allowing a single, golden source of data to be used across everything from client presentations to fund centers and beyond. This lowers compliance risk, reduces integration costs, and increases the ability of the firm to meet the ever-increasing challenges posed by investors, regulators, and competitors.

Founded in 2002 and headquartered in London, Kurtosys serves some of the world's largest asset managers. Find out more about our full range of solutions at www.kurtosys.com.

FOLLOW US

WWW.KURTOSYS.COM