

KURTOSYS

Real growth. Realized.



Standard Support Promise

June 2020

WWW.KURTOSYS.COM

STANDARD SUPPORT PROMISE

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.

Support

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:

- Date & time of incident
- Contact name(s) for follow-up
- Your incident classification (critical (P1), major (P2), minor (P3) – defined below)
- A description of incident
- A description of impact to service
- The user details/URL used to access the product and service when the incident occurred
- Steps on how to reproduce the incident
- 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.

For P1 incidents out of standard helpdesk support hours, please call: **+1-646-503-5601**.

Most P1 incidents will be detected by our monitoring and will automatically be escalated internally.

Out of Hours

Our internal systems automatically monitor our services and underlying servers. Other than this, we do not provide out of hours support via the service desk.

- Kurtosys uses monitoring technology to evaluate availability.
- Critical platform outages will automatically be escalated internally.
- Out of hours tickets from you are routed to a central call center or 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.

Incidents

Definition: Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Measured against service level metrics.

Incident Management

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

- All critical incidents (P1) and major incidents (P2) that impact five (5) or more customers, that involve the platform for delivery which are fifteen (15) minutes or longer will have an incident report delivered within 7 days.
 - Any incident that involves a security breach will result in immediate notification and follow our security Incident Response Plan
 - The incident report will contain a root cause analysis and remediation.
 - If a root cause is identified, it may be shared earlier by email/phone.
 - For other types of errors, a root cause can be supplied if requested.
- 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.

Incident Priority Summary:

Priority	First Response	Restore
Critical P1	1 Hour	4 Hours
Major P2	2 Hours	8 Hours
Minor P3	8 Hours	As agreed

Critical Incidents (P1)

You are encountering a critical issue, which means that the platform is not available and productivity has been halted. The product is unusable in its current state.

- We aim to acknowledge 95% of critical incidents within one (1) hour of receipt of your ticket being logged.
- We aim to provide a solution to 95% of critical incidents within four (4) hours of acknowledging your notification.
- We will provide updates every thirty (30) minutes to share our efforts to resolve the critical incident and an estimated resolution time if known.
- If we become aware of a critical incident, we will notify you within one (1) hour and keep you updated as to its resolution.

- If you become aware of a critical incident, please send an email to support@kurtosys.com, or log a ticket using the service desk customer portal or call us following the process outlined in the "Support" section above.
- Our support team will acknowledge your notification via email.
- If we cannot provide a solution or work-around within four (4) hours and the incident is related to an infrastructure or data-centre issue, we may invoke the disaster recovery plan.
- On a case-by-case basis, we may both agree to a reasonable extension of the response, resolution, and reporting commitments cited above.
- An example of a P1 issue would be the unavailability of an entire website (in other words, no pages are responsive) or more that 50% of the websites, or where parts of a website which are a regulatory requirement are unavailable and no workaround is available. An additional example would be the unavailability of the entire platform or more that 50% of the platform.

Major Incidents (P2)

You are encountering a major issue, which means that the system is available, albeit you are experiencing issues that have a direct impact on productivity and day-to-day activities. Major inconvenience.

- We aim to acknowledge 95% of major incidents within two (2) hours of receipt of your notification.
- We aim to provide a solution in respect of 95% of major incidents within one (1) Business Day of acknowledging your notification.
- We will provide updates everyone (1) hour to share our efforts to resolve the Major Incident and an estimated resolution time, until the resolution time is confirmed.
- If we become aware of a major incident, we will notify you within two (2) hours and keep you updated as to its resolution.
- If you become aware of a major incident, please send an email to support@kurtosys.com or log a ticket using the service desk customer portal and assign the appropriate level of severity.
- Our support team will acknowledge your notification via email.
- Solutions and work-around(s) will be provided during support hours.
- On a case-by-case basis, we may both agree to a reasonable extension of the response, resolution, and reporting commitments cited above.
- An example of a P2 incident would be where a section of a website is unavailable. A further example would be the unavailability of up to 50% of the functionality on the platform.

Minor Incidents (P3)

You are encountering a minor issue, which means that the platform is having an occasional issue that has been identified as needing to be resolved, but the issue has not greatly affected productivity. Minor business inconvenience.

- We aim to acknowledge 95% of normal incidents within eight (8) hours of receipt of your notification during support hours.
- We aim to provide a solution of normal incidents within a timeframe reasonably agreed with you.

- If you become aware of a normal incident, please send an email to support@Kurtosys.com or log using the service desk customer portal.
- We will acknowledge your notification during support hours via email.
- Solutions and work-around(s) will be provided during support hours.
- On a case-by-case basis, we may both agree to a reasonable extension of the response, resolution and reporting commitments cited above.
- An example of a P3 incident would be a formatting or styling error on a document of web page created using the Kurtosys platform, which is not detrimental to the conveyance of the required information, but which is not in line with the agreed to specifications.

Classification

We expect you to indicate the incident classification, however we reserve the right to re-classify according to the incident characteristics stated above.

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



Priority Classification Matrix Diagram

Definitions to assist with classification:

Impact measures the effect of an incident on business processes. We can evaluate the impact based on several criteria:

- The number of affected users.
- The potential for financial loss.
- The number of affected services.
- Breaches of compliance, regulations or laws.
- Effect on the reputation of the company.

Urgency is usually defined when more than one service is impacted, parameters for the higher urgency service will be taken into account.

- A period where a system is considered as more critical (for example, the routine creation of regulatory documents which occurs at a certain schedule within the month)
- When some systems are identified critical with a high availability level (for example; regulatory documents, daily pricing information, or legal disclaimer content)

Priority is based on impact and urgency and is used to identify the speed of the response and resolution.

- The allocation of a priority code determines how the incident is being addressed by the support team. Using the fields impact and urgency is optional to obtain a priority.

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.

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

Platform System Monitoring

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

- Our services (applications, databases, servers, network, etc.) are monitored.
- All alerts are logged and distributed by our monitoring and alert systems.
- Multiple levels of monitoring consist of: Data Monitoring, Infrastructure Monitoring and User Interface Monitoring.
- Our technology and support teams are automatically notified of an event or incident via our regular communication channels.

Service Requests

Definition: 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.

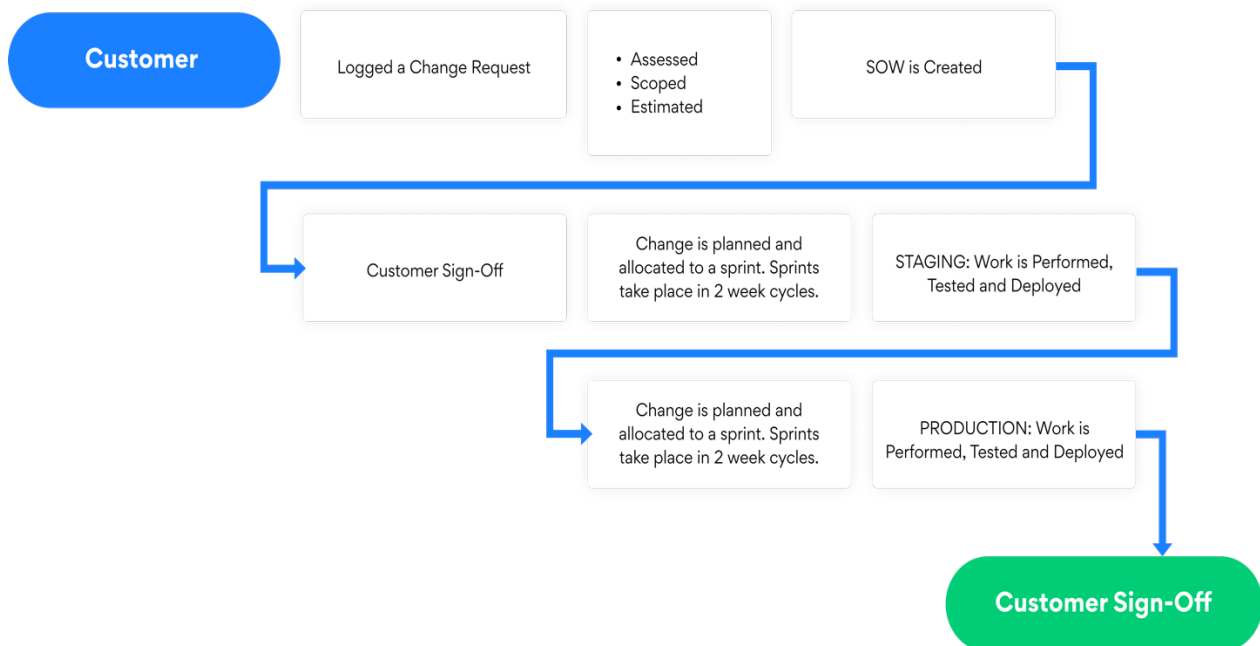
Service Requests are not subject to measurement against service level metrics.

Changes

Definition: 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.

Change Request Process



Process Diagram: High-level change request process

Platform Change Management

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

- Our Change Management Board (CMB) meets twice weekly; all changes reviewed are tracked for reporting purposes.
- CMB ensures changes are documented, tested, resourced, and a rollback plan is in place.
- CMB includes an approval process and escalation for emergency changes.

Reporting

Quarterly Reporting

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

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

Incident Reporting

Platform incidents:

- All critical incidents (P1) and major incidents (P2) that impact five (5) or more customers, that involve the platform for delivery which are fifteen (15) minutes or longer, will have an incident report delivered within 7 days.

Customer Impacting Incidents:

- Critical (P1) incidents that impact on the Platform will have an incident report delivered within 7 days.

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.

- We have implemented ISO 27001 which is certified by an external auditor annually. This includes an ISMS and comprehensive security that determines how we operate, as well as how we classify and handle data.
- We use Cloud based IaaS (Infrastructure as a Service) provided by certified vendors in resilient and secure data centers within appropriate data jurisdictions.
- 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.
- We apply WAF (Web Application Firewall), DDoS (Dynamic Denial of Service) and other IDS/IPS protection to all network traffic.
- We have Risk Assessment and Vulnerability Management programs to confirm our security controls are effective.

Disaster Recovery (DR)

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

- 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.
- Backups are stored daily for one (1) week and are then available for one (1) month.
- Standard DR is based on a rebuild of the last backup, restored into the appropriate standby environment in the same data jurisdiction.
- Recovery time objective (RTO - https://en.wikipedia.org/wiki/recovery_time_objective) is four (4) hours.

Capacity Management

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

- Capacity management is handled at the platform level.
- Our platform is horizontally and vertically scalable to maximise operational availability.
- Data loading is monitored to ensure operational integrity.
- Our Cloud Infrastructure providers have Service Level Agreements and certifications for provisioning and service delivery.

Out of Scope

All other support services are out of scope.

- 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.
- 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.

About Kurtosys

Kurtosys empowers financial services firms to create powerful investor experiences and lasting customer relationships through efficient automation of key sales, marketing and customer service processes.

The company provides an end-to-end digital experience platform (DXP) that enables firms to create, manage, publish and optimize all their financial data, documents, websites and content in a secure, compliant environment.

As a result, it is trusted by the world's leading investment brands to mitigate their risks and reduce their costs while providing the agility to ensure they are first to market.

Kurtosys solutions include secure websites and portals, interactive data tools and apps, automated sales presentations, marketing collateral and reporting and document libraries.

Kurtosys architecture is underpinned by robust and scalable infrastructure using the latest Cloud technologies and supported by teams that understand information design, industry regulations and compliance issues and working at scale with data.

We are an ISO 27001 certified company. We have implemented a comprehensive information security management system to protect customer services including Data Centre protection, business continuity, risk assessment and incident management.

Founded in 2002, Kurtosys was funded from Silicon Valley investment and operates across three global offices, employing over 200 people. The company works with some of the world's largest financial brands, including banks, wealth managers, mutual fund providers and alternative investments.

Contact Kurtosys

Whether you're a bank, private equity firm or an asset manager, looking to build a brand-new website, client portal or product campaign, or whether you just need to improve your data visualization or get your marketing documents out faster – get in touch!

Visit www.kurtosys.com to learn more.

Visit www.kurtosys.com/contact to request a free demo.

KURTOSYS**Real growth. Realized.**

London, United Kingdom
+44 (0)800 0291410
77 Kingsway, 1st Floor,
London, WC2B 6SR,
United Kingdom

Cape Town, South Africa
+27 (0)80 099 8415
Mont Clare Place, 2nd Floor
35 Main Road, Claremont 7708,
South Africa

Raleigh, United States
+1 844 566 5331
5171 Glenwood Ave, Suite 460,
Raleigh NC 27612,
United States

Copyright © 2020 Kurtosys Systems. All rights reserved.