

KURTOSYS

Pain-free investment data
and insight delivery

SUPPORT PROMISE

prepared by Natalie Kennedy, Head of Client Service

1. INTRODUCTION	3
2. DEFINITION OF TERMS	3
3. SUPPORT PROCESS	4
a. Standard Support Hours	4
b. Logging a ticket	4
c. Out of Hours Support	5
4. INCIDENTS	5
a. Incident Management	5
b. Priority and Service Levels for Incidents	6
P1 Status (Critical)	6
P2 Status (High)	6
P3 Status (Medium)	6
c. Incident Classification	7
d. Service Level Credits	7
5. SERVICE REQUESTS	7
6. CHANGE REQUEST	8
a. Change Request Process	8
7. PLATFORM	9
a. Platform Availability	9
b. Platform System Monitoring	9
c. Platform Change Management	9
8. REPORTING	10
a. Quarterly Reporting	10
b. Incident Reporting	10
9. SECURITY	10
10. BUSINESS CONTINUITY AND DISASTER RECOVERY	10
11. CAPACITY MANAGEMENT	11
12. OUT OF SCOPE	11
13. ABOUT KURTOSYS	12
14. CONTACT KURTOSYS	12

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.

This Service Level Agreement may be modified by Kurtosys from time to time, with 7 days prior notification to the client. Amendments to the Service Level Agreement will be non-material. Non-material is to be understood as not interfering, either directly or indirectly, with neither the quantity nor the quality of service to be delivered by Kurtosys towards the client. Any amendments will be specifically to clarify or add to specific items.

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. The definition of an Incident is not limited to any specific cause or event. For the avoidance of doubt, Application errors, errors due to erroneous data in files and unanticipated interactions of configuration are considered as an Incident. In other words, any unexpected event, not part of the standard behaviour that would cause an unplanned interruption to a service or reduction in the quality of the service.
- c. **Service Request** is a request from the client for our Support Desk to perform an activity on behalf of the client.
- d. **Change Request** is an instruction from the client to make a change or addition to existing functionality
- e. **Change Control** is the Kurtosys process for proposing and approving alteration to an existing implementation or system functionality
- f. **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.
- g. **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
- h. **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**.
- i. **Remediation** is the process of correcting the effects of the **Incident**.
- j. **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

- k. **Progress Report** is the interim report provided to the client by Kurtosys only for Incident classified as P1 which documents (if available at the point in time):
- Incident number
 - Description of the incident
 - Root cause of the incident
 - Potential workaround
 - Description of the solution applied
- l. **Acknowledgement** is the initial notification added to a **Support Ticket** confirming receipt of a reported **Incident**.
- m. **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

Kurtosys will provide standard Service Desk services between 08:00 GMT (08:00 UTC) and 15:00 US PST (23:00 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.

We are expanding the team (to be in place by end June 2023) that will provide standard Support Desk services until 17:00 PST and be allocated to US and APAC specific clients to provide more focus and efficiency for clients in that geographical location.

b. Logging a ticket

If you have an Incident, Service Request or Change Request, please contact our Service Desk by logging a ticket via the Service Desk Client portal. Each client user will receive a login to the Service Desk portal before Production. These login credentials will provide access to log a ticket, view ticket status & communications and view various reports.

If the client cannot log a query via the service desk, they should send an email to support@kurtosys.com which creates a ticket within our Service Desk. This however, needs to be used as secondary measure as we cannot validate all required fields from an incoming email.

When logging an Incident, it should contain, when possible, the following information:

- i. Date & time of incident
- ii. Contact name(s) for follow-up
- iii. Your incident classification (P1/Urgent, P2/High, P3/Medium) – 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. On the 3rd day, Kurtosys will send a reminder to the client indicating that if no feedback is received then the ticket will be closed within 24 hours. Tickets which receive no feedback from the client for 3 consecutive business days, will prompt an automatic closure on the service desk.

c. 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 within our Standard Support hours, 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 the Service Desk, the issue will be logged and responded to on the next business day, unless the incident is a P1 incident in which case the Support Team are notified for a P1 response.
- iv. Note that these tickets should contain the phrase “P1” to be picked up by our system
- v. An on-call rota system operates for critical and emergency notifications to our Support Team.

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 P3 incidents, a root cause will be supplied by Kurtosys if requested by the Client.
- vii. Application errors, errors due to erroneous data in files, and unanticipated interactions of configuration will be classified accordingly to clarify the explanations given in Incident Reports.

b. Priority and Service Levels for Incidents

The Priority Status is initially defined by the client and will be evaluated and agreed upon by Kurtosys should the incident meet the required criteria. Any decrease in priority would need to be done in agreement with the Client.

P1 Status (Critical)

Definition	This definition covers any of the following: <ul style="list-style-type: none">i. Entire platform/service is down and unavailableii. The problem results in compliance, regulatory or financial liability due to operational or informational deficiency.iii. A security breach has occurred resulting in loss of data or control of the application.
Acknowledgement	< 1 hour.
Ticket update frequency	Approx. 30 mins
Remediation or mitigation	< 4 hours from the logging of the incident ticket
Incident Report	5 business days from remediation
Progress Report	2 business days from Incident. An email shall be sufficient

P2 Status (High)

Definition	The platform/service is available but with issues that have a direct impact on productivity and performance of day-to-day activities. A major component of the client's ability to operate is affected. Some aspects of the business can continue and there is no compliance risk, but there is a risk of damage to brand / reputation.
Acknowledgement	< 2 hours
Ticket updates frequency	Approx. 60 mins
Remediation or mitigation	< 8 hours from Acknowledgement
Incident Report	5 business days from remediation or as agreed between parties

P3 Status (Medium)

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.
Acknowledgement	< 2 hours
Ticket updates frequency	1-3 days as ticket specifics require
Remediation or mitigation	3-5 days or as agreed between parties
Incident Report	As appropriate, upon request from the Client

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 (only in agreement with the Client if the priority is to be decreased), 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 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 escalate our responses properly and fairly and to provide a better service to all our clients.
- 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 may subject to:

- i. Different incident types
- ii. Duration of Outages
- iii. Frequency of Incidents
- iv. Incident remediation and reporting
- v. Etc

The specific Credit Levels may be issued as an Appendix to the Main Client Agreement.

5. 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, and we will assist our clients by means of a self-help guide. We request that clients undertake the changes to be made upon themselves as this enables clients to understand the platform better and frees up our Service Agents to focus on Incident Management.

6. Change Request

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 client wants an addition or alteration to the agreed-upon deliverables.

Changes are not subject to measurement against service level metrics.

The Change request will be coordinated by your Client Service Manager as part of each clients' operational requirements.

a. Change Request Process

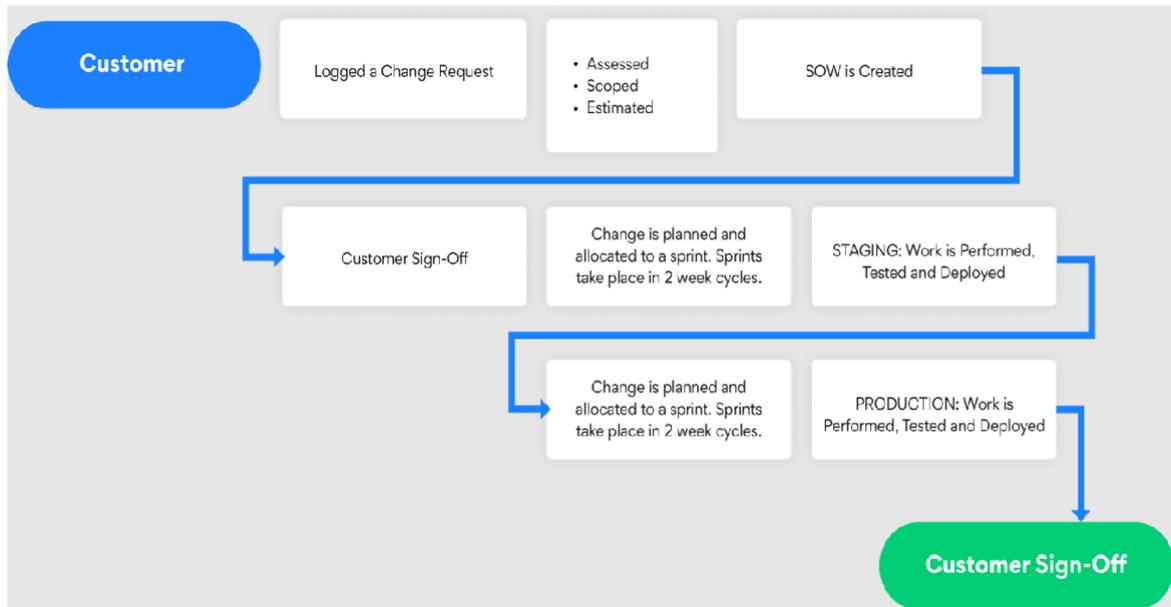


Figure 1: Process Diagram: High-level change request process

7. 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 (UTC) weekdays and between 01:00 (UTC) Saturday and 23:00 (UTC) Sunday weekends, provided that the client has been duly informed in advance.
- 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.

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

- i. All alerts are logged and distributed by our monitoring and alert systems.
- ii. Multiple levels of monitoring consist of: Data Monitoring, Infrastructure Monitoring and User Interface Monitoring.
- iii. Our technology and support teams are automatically notified of an event or incident via our regular communication channels.

c. 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.

8. Reporting

a. Quarterly Reporting

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

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

b. Incident Reporting

All incident reports for P1 & P2 level incidents 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.

9. 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 on an annual basis. This includes an ISMS that implements all of the recommended 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

10. 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 in our Business Continuity Plan.

- 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.

11. 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.

12. 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 Client 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.

13. 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 global offices, employing around 200 people. The company works with some of the world's largest financial brands, including banks, wealth managers, mutual fund providers and alternative investments.

14. 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.

London 86-90 Paul Street 3rd Floor London EC2A 4NE	Luxembourg The LHoFT, 9 Rue du Laboratoire, 1911 Luxembourg	Cape Town Mont Clare Place, 35 Main Rd, Claremont 7708, South Africa
---	--	---