INCIDENT MANAGEMENT & INFRASTRUCTURE SUPPORT POLICY

INCIDENT MANAGEMENT SERVICES

CAPITALIZED TERMS HEREIN THAT ARE NOT OTHERWISE DEFINED SHALL HAVE THOSE MEANINGS ASCRIBED TO THEM IN A LICENSE AGREEMENT BETWEEN BEACON PLATFORM INC. ("BPI") AND A LICENSEE (EACH A "LICENSE AGREEMENT").

Subject to the payment of Infrastructure and Incident Management Fees Beacon provides its Licensees with the incident management services and infrastructure support specified in this Incident Management & Infrastructure Support Policy (the "Incident Management Services"). Incident Management Services are made available with respect to the BPI MATERIALS only and are not made available with respect to any of the following: (i) Licensee Usages; (ii) custom development of the Platform performed by or on behalf of the Licensee; (iii) general training requests; (iv) question and answer sessions initiated by Licensee; (v) Licensee enhancement requests; and (vi) Licensee-Created Issues (as defined below). Any such Additional Services shall be separately chargeable in accordance with BPI's then-current time and materials consulting rates.

A. **Requests for Support:** All requests for Incident Management Services must be made through the BPI Incident Management Tool.

BPI responds to all formally submitted requests for Incident Management Services by conducting an initial analysis of a request from a Licensee clearly outlining the precise details of the underlying issue and the necessary context and a reproducible case wherever possible, including as much information as is capable of being shared with BPI regarding the underlying issue. In addition, in order for BPI to investigate the underlying issue, a Licensee must grant to BPI the sufficient authority and rights of access necessary for such investigation. Based on Licensee's input and BPI's investigation, BPI will confirm whether the underlying issue is one for which Incident Management Services are appropriate and will prioritize and respond to Licensee's request in accordance with the Severity Levels and Initial Response Times described below.

B. **Incident Prioritization; BPI Response:**

1. Definitions: :

(a) "Business Day" means any day except any Saturday, any Sunday, any day that is a federal legal holiday in the United States, any day that is an official BPI company holiday, or any day on which banking institutions in Licensee's Primary Support Location city are authorized or required by law or other governmental action to close.
(b) "Business Hour" means any sixty (60) minute period of time on a Business Day between the hours of 9:00am and 5:00pm in Licensee's Primary Support Location.
(c) "Initial Response Time" shall mean the amount of time between the time a Licensee logs a ticket through the BPI Incident Management Tool and when BPI acknowledges receipt of such ticket.
(d) "Primary Support Location" shall have the meaning ascribed to it in a License Agreement
(e) "Resolution Time" shall mean the amount of time required by BPI to address and resolve a request from Licensee for Incident Management Services; provided that such Resolution Time shall not begin to accrue until (i) BPI has been given all of the information necessary for BPI to resolve the issue, and (ii) Licensee has granted BPI access to the Licensee's Domain.

2. Incident Prioritization and Initial Response Time: Using the information provided by a Licensee and based on BPI's information and initial investigation, BPI will assign one of the following "Severity Levels" to the issue underlying the request for Incident Management Services. BPI's designation of the Severity Level will dictate the required Initial Response Time :

(a) "Severity Level 1" (Blocker): *All of Licensee's Permitted Users are unable to access the Platform.*

Support Tier	**Initial Response Time**	**Resolution Time**
Platinum	1 hour (24/7)	4 Business Hours
Gold	1 Business Hour	None
Silver	4 Business Hours	None
Bronze	Reasonable Time Frame	None

(b) "Severity Level 2" (Critical): *An incident that materially impairs the Platform's performance, functionality, or availability with the consequence that business operations can be performed but in a very restricted or inefficient manner, e.g. some of Licensee's Permitted Users are unable to log into the Platform, some of the Licensee's applications on the Platform are failing, critical batch jobs on the Platform are failing, or Licensee is unable to release new code on the Platform.*

Support Tier	**Initial Response Time**	**Resolution Time**
Platinum	1 Business Hour	None
Gold	4 Business Hours	None
Silver	4 Business Hours	None
Bronze	Reasonable Time Frame	None

(c) "Severity Level 3" (Major): *An incident that impairs the Platform's performance, functionality, or availability, but does not cause a material impact on business operations, e.g. a non-critical batch job is failing or the availability or functionality of a non-critical application or tool (such as Plot Tool, Grafana, or the Excel Add-In) is impaired.*

Support Tier	**Initial Response Time**	**Resolution Time**

Platinum	8 Business Hours	None
Gold	8 Business Hours	None
Silver	24 Business Hours	None
Bronze	Reasonable Time Frame	None

(d) "Severity Level 4" (Minor): *An incident that impairs the Platform's performance or functionality but does not cause a material impact on business operations, yet the performance or efficiency of the Platform might improve if the incident were to be corrected, e.g. any issue with the Documentation or application issues related to a single Permitted User, issues with documentation, or non-disruptive issues impacting a Beacon component or Beacon-provided app.*

Support Tier	**Initial Response Time**	**Resolution Time**
Platinum	24 Business Hours	None
Gold	24 Business Hours	None
Silver	Reasonable Time Frame	None
Bronze	Reasonable Time Frame	None

C. **Supported Releases:** BPI will provide Incident Management Services in accordance with the terms of this policy and the applicable License Agreement for so long as a Licensee's then-current version of the Platform is up-to-date or within two (2) prior releases of the up-to-date release (the "Release Support Window"). If, at any time, a Licensee's then-current version of the Platform falls out of the Release Support Window, then BPI's Incident Management Services obligations will be suspended until such time as such Licensee accepts a then-supported release of the Platform.

D. **Licensee-Created Issues**: Time spent by BPI investigating any issues that are determined to have been created due to the acts or omissions of Licensee or its Affiliates, including, but not limited to: (a) modification of the object code of the Platform; (b) improper manipulation of data via a derivative work; (c) improper manipulation of data via an interface or integration with another software product or internally developed computer system; (d) improper conversion of data from an existing legacy system into the data structures; (e) combining or merging the Platform with any hardware or software not identified by BPI as compatible with the Platform; or (f) overloading shared infrastructure services and/or mismanaging capacity issues (each, a "Licensee-Created Issue" and, collectively, the "Licensee Created Issues") will be billed separately at BPI's then-current standard consultancy rates as Professional Services and are outside the scope of Incident Management Services.

E. Licensee’s Expert Users: Each Licensees will designate in writing at least one (1), and up to three (3), of its personnel (each, an “Expert User”), who will have direct contact with BPI and only such Expert Users will have the right to contact BPI directly regarding Incident Management Services. Expert Users are responsible for performing initial triage to determine whether an issue is a Licensee -Created Issue. Each Licensee will have the right in its sole discretion to replace a designated Expert User, and upon replacing an Expert User, Licensee will provide prompt written notice to BPI as to which Expert User has been replaced and the name of the new Expert User replacing the former Expert User. In the event a Licensee elects to increase the number of Expert Users, in excess of the quantity permitted, then Licensee and BPI will mutually agree on appropriate fees for such increase in the number of Expert Users.

INFRASTRUCTURE SUPPORT

In consideration of a Licensee's payment of the Infrastructure and Incident Management Fee specified in the License Agreement, and subject to a Licensee's adherence to and implementation of BPI's reasonable infrastructure recommendations as communicated by BPI to such Licensee from time-to-time, BPI provides such Licensee with the Infrastructure Support Services set forth below. BPI's obligation to provide the Infrastructure Support Services in the table available in the BPI RACI. (and including, without limitation, the installation services described in the License Agreement) shall be subject to a Licensee making its environment available to any one or more of BPI's support personnel.

Infrastructure Management:

1. BPI manages infrastructure using software, allowing for automated and replicable infrastructure management.
2. All compute capacity is provided in a Licensee's segregated single tenant, client-specific cloud provider account.
3. For PaaS Licensees, it is a Licensee's obligation to reserve long-term, always-on infrastructure (such as database servers) from their cloud provider. BPI may provide details of server sizing for Licensee's reservation. For SaaS Licensees, BPI passes through the cost of such infrastructure to Licensee.

Environment Availability:

BPI commits to an availability for each Licensee of no less than the Licensee's Environment Availability Percentage in any given month during Business Hours for such Licensee's Critical BPI Components (as defined below) ("Environment Availability").

Downtime resulting from the following shall not count against the availability commitment for any Licensee's Critical BPI Components.

- Cloud provider downtime or scheduled maintenance
- Outages caused by misuse of the platform by a Licensee
- Failure of the Internet and/or public switched network
- Emergency maintenance to correct or protect against significant security vulnerabilities or other catastrophic issues
- Downtime occurring during an agreed upon maintenance window approved by both BPI and a Licensee

"Critical BPI Components" are defined as only such infrastructure and services that are essential to allow for computation to be performed on the Platform. If the Critical BPI Components are operating, then the Platform is considered "available."

Disaster Recovery: (Only available per a Licensee's License Agreement.)

1. BPI Object database backends ("MongoDB") can be replicated across multiple instances in independent cloud provider Availability Zones (each, an "AZ");
    a. Database failover is delegated to MongoDB replication sets, which can be configured to automatically elect a new master.
    b. BPI commits to addressing affected infrastructure within one (1) Business Day of notification of the issue, excluding any time during which the Licensee's cloud provider is experiencing a service outage.
2. Upon request from a Licensee during implementation of the Platform, BPI will replicate MongoDB across multiple AZs. Such replication will incur additional cloud provider data costs for such Licensee. BPI commits to executing its disaster recovery process for an AZ failure within one (1) Business Day of notification of the issue, excluding any time during which a cloud provider is experiencing a service outage.
3. Single compute resource failover is automatic and transparent to the Licensee, and occurs according to the following parameters:
    a. New compute resources are automatically spun up to the capacity agreed with the Licensee;
    b. The "Bob" batch job scheduler automatically reschedules batch jobs from failed compute resources to others in the elastic compute pool. Jobs that are ongoing at the time of failover may fail and require some manual intervention by Licensee to reschedule onto new compute resources;
    c. The WMP (WST Multi Processing) grid scheduler automatically reschedules parallel compute jobs from failed compute resources to others in the elastic compute pool. Repeated failures may need to be addressed by Licensee via manual intervention.

Data Backup:

1. By default, Beacon's object database backend (MongoDB) is fully replicated between primary and secondary nodes hosted in different cloud provider Availability Zones.
2. All persistent data volumes for all servers in a Licensee production environment are snapshotted using cloud provider snapshot technology daily by default. A Licensee may change the frequency of snapshots or exclude servers from snapshots.
3. Data stored in the cloud provider's object storage is subject to cloud provider availability.
4. BPI never deletes trade data; it is stored in the MongoDB: BPI keeps an audit log of all trade actions and events.

Security:

1. All persistent data stored on Block Storage is encrypted at rest in line with the cloud provider's standard & best practice. Encryption keys are managed by the cloud provider and are unique per Platform installation. Where supported by the underlying cloud provider, a Licensee's Platform installation may leverage Customer Managed Keys for Block Storage encryption.

2. BPI Services encrypt any external data transfers over SSL/TLS using a key that is unique to each Platform installation. Internal traffic will be encrypted according to BPI's standards available here.

Additional Infrastructure:

In the event BPI reasonably determines that a Licensee’s Platform requires additional cloud infrastructure, BPI may provision such additional infrastructure on such Licensee’s behalf.

Elastic Compute:

1. Computing capacity (batch jobs, parallel compute, application back end processes, Excel interface backends, etc.) is increased or decreased dynamically as required (“Elastic Compute”)
2. Elastic Compute pools are defined with minimum and maximum number of available cores, with ability to define available core numbers on a schedule
3. Elastic Compute costs are minimized through automated management of Elastic Compute pools, leveraging cloud provider “on-demand” instances for critical tasks and can take advantage of cloud provider “spot” instances for non-critical tasks. The decision of whether to use “on-demand” or “spot” instances will be made by each Licensee.

Database Usage:

The object database backend is delivered with the Platform for ancillary use only via BPI-provided APIs and is not permitted to be used by Licensee as a standalone service. In the event a Licensee wishes to utilize the object database backend directly or otherwise utilize the object database backend as a primary service, each Licensee must obtain a license for such use directly from the licensor of the object database backend or from Licensor if Licensor is an approved reseller of the object database backend.