Business Continuity Plan

Hapi Corp. ("Hapi") has worked and improves periodically it business continuity with any update or new technology available and added to their stack. The following include but do not limit the actions Hapi takes to continue its operations in case of any disaster.

1) Alerts in Place

Hapi has a series of automatic alerts in place to monitor and supervise the correct performance and functioning of its platform. The alerts are triggered automatically when any system is down, and depending on the severity of the problems, different responsible in a chain of command are notified so further actions can be taken.

Alerts are segmented by each particular system for identification of the issues, the compromise modules, and if it is an internal or external issue, allowing Hapi for a subsequent quicker resolution.

2) Systems Automatic Restorations

Hapi business continuity and disaster recovery plan triggers after getting an alert that the system is down. Hapi addresses wherever the problem is internal or external.

For external system breaks, reviews are done about connectivity and actual status of the external system. Hapi mitigated external systems downtime by selecting top tier suppliers that after due diligence and screening provide compelling infrastructure that is robust and reliable to Hapi standards.

In the case of connectivity and Hapi's internal platform has an always on infrastructure that provides a near seamless continuity in case of failure (or multiple failure). Hapi's platform and technology has been built including redundancy in case of failure, when a system fails, next one takes over with no downtime, and the one that failed automatically restarts, restores, and runs within minutes. If all systems fail this will automatically restart and restore within minutes.

3) Continuity Plan

Hapi is a remote company, with no physical offices, all its information, infrastructure and systems are hosted on the cloud, and thus in a case of an act of god cannot be compromised.

Regarding third party service providers, there can be split in critical (clearing firm) and non-critical (all the rest). Non-critical providers downtime translates in a less optimal experience for Hapi users but do not

mean a break in operations continuity. For the case of the critical external service provider, the clearing firm, Hapi selected one of the best clearing firms available, a first level trust worthy, experienced and robust one; Hapi's clearing firm employs technology architecture that focuses on continuity, which allows them to be unaffected by the vast majority of potentially catastrophic localized events. They maintain multiple data centers, both for their physical infrastructure and software infrastructure, whereas if an event occurs that threatens their infrastructure, any one data center can take over all their critical and necessary functions with little or no intervention, they are always available and highly fault tolerant.

4) Major breakdown

In the case of a major event, the immediate concern for Hapi is the safety of its team. Once employees have been secured, Hapi will identify the scope of the incident. If systems have been critically compromised one of Hapi's officers will assess the damage, determine the estimated length of the outage, and instruct following procedures for the rest of the organization to follow, including a public statement for users via email and social media outlets. In the event of a breakdown and you wish to contact us directly, please email us at contacto@imhapi.app or through and of our social media channels.