Pegasus Cloud Service Level Agreement

Infrastructure - The services are supported by commercially reasonable redundant infrastructure including

- Power infrastructure that includes redundant sources (multiple power feeds, generators, battery backups), multiple power distribution systems, and redundant power supplies;
- Environmental controls that include highly available precision HVAC systems, humidity controls, and water detection systems;
- Network infrastructure that includes multiple Internet Service Providers, redundant edge routers, firewalls, and switches;
- Hardware and software redundancy in support of virtualized and physical servers; and
- Storage solutions that provide redundant back end data storage.

Our platform provider maintains a disaster recovery site where Licensee's data is replicated on a regular basis.

Technical Change Management - Our platform provider maintains change management system to ensure review and controlled implementation of changes that our platform provider may make from time to time in the support of the services. Changes require both a risk analysis and a peer review before being implemented in our platform provider's infrastructure.

Security & Privacy - Our platform provider takes great care to protect non-public information provided to us by our customers. Our platform provider may have access to non-public information from multiple sources that include:

- Directly from use of one of Intsys hosted applications.
- Directly from a customer's designated service representative or indirectly via batch data transfers.
- In the course of transactional activities as information is updated or processed by an Intsys hosted application, or through data maintenance activities.
- Other sources as defined by one of our solutions.

Our platform provider has implemented a defense-in-depth strategy to protect non-public information. This strategy is based upon best-practices designed to comply with applicable laws and regulations and is based upon widely accepted industry standards. Our security management system is based on the following:

- Security Policies: We require that all employees be responsible for the security of non-public information and follow the practices defined within the Information Security Management System.
- Information Security Organization: Our platform provider's management is committed to security and has established an organization responsible for the security of non-public information.
- Asset Management: All assets are strictly controlled and all information is classified in order to determine the appropriate controls required for access and handling.
- Human Resources Security Practices: Our platform provider requires that employees maintain familiarity and compliance with security responsibilities. When employees leave Our platform provider, a formal process is established to remove their physical and virtual access to the infrastructure.
- Physical and Environmental Security: Our platform provider places critical components in physically controlled spaces with best-practices in place to secure infrastructure. Physical and environmental security measures include card and/or biometric access controls, and limited access to secure locations based on job function.
- Communication and Operations Management: Our platform provider has implemented strong operational procedures to protect information. Our controls surrounding system planning, protection from malicious code, backup processes, network security, media handling and exchange of information are constantly being analyzed and monitored to insure they provide reasonable protection for your data. Third party service providers with access to confidential information are required to adhere to security and privacy requirements that are consistent with and at least as restrictive as Our platform provider's own policies and procedures regarding the protection of confidential information.

- Access Control: All access to systems, networks, and applications is controlled down to the user and resource level with role-based privilege techniques. This access is reviewed on a periodic basis to ensure that a change of personnel or a change of role has not modified the access needs of the individual.

- System Development: Security requirements of all applications that handle confidential information are defined early in the development stage. Appropriate data protection techniques are designed into the application while changes to developed software must go through a mature change management process.

- Incident Management: In the unlikely event of an actual or reasonably suspected security incident, our teams immediately begin work to identify the scope of impact, mitigate any exposure, determine the root cause of the incident and take appropriate corrective action.

- Compliance: We are constantly analyzing the requirements of legal, regulatory, and contractual obligations to ensure we are abiding by the requirements that apply to the handling of your data.

Scheduled Maintenance - The services shall be subject to a regularly scheduled weekly maintenance window. Our platform provider makes commercially reasonable efforts to establish maintenance windows during times that minimize impact to Licensee's users. While most of Our platform provider's maintenance can be completed during regularly scheduled maintenance windows, from time to time maintenance must be performed outside of the scheduled maintenance windows to maintain the integrity and security of the services. In such cases, our platform provider will provide Licensee's primary point of contact as much advance notice of the planned maintenance as is technically feasible. The regularly scheduled weekly maintenance windows and any period of unavailability due to maintenance for which Licensee is given at least 24 hours advance notice is considered "Scheduled Maintenance".

Availability - Our platform provider's goal is to provide access to the services at our platform provider's Internet gateway(s) twenty-four hours per day, seven days a week, except during Scheduled Maintenance. Our platform provider's service level objective is 99.5% Availability measured on a monthly basis.
Availability for the Subscription Services is measured monthly as a percentage of Scheduled Available Minutes.

- "Scheduled Available Minutes" are the total minutes in a month less the number of Scheduled Maintenance minutes in the applicable month.

- "Available Minutes" is the number of Scheduled Available Minutes in a month less the aggregate number of minutes the Subscription Services were unavailable outside of Scheduled Maintenance.

- "Availability" is a percentage calculated as the Available Minutes in a month divided by the Scheduled Available Minutes in the month.

For example, in a 30 day month with 4 weekly Scheduled Maintenance windows of 8 hours, there are 41,280 Scheduled Available Minutes ((60 min. x 24 hrs. x 30 days)-(60 min. x 8 hrs. x 4 weeks) = 41,280). If the Subscription Services experienced an outage of two hours outside of Schedule Maintenance, there were 41,160 Available Minutes in the month (41,280 Scheduled Available Minutes – 120 minutes of unavailability). The resulting Availability percentage is 41,160 / 41,280 = 99.7%.

The following shall not be considered periods of unavailability for purposes of the Availability calculation:

- Outages due to factors outside of our platform provider's reasonable control (for example, a network or device failure at Licensee's site or between Licensee and Our platform provider's data centers);

- Delays in email or webmail transmission to or from the hosted application;

- Connectivity issues outside of our platform provider's direct control (e.g. DNS issues);

- Force Majeure events;

- Outages attributable to the acts or omissions of Licensee or Licensee's employees, agents, contractors, or vendors, or anyone gaining access to the services means of User IDs or equipment controlled by Licensee;

- Periods of Down Time at Licensee's request;

- Outages that result from Licensee's equipment, software, or other technology and/or third party equipment, software or other technology (other than those which are under Our platform provider's direct control); and

- Performance degradation due to Licensee's use of the services in excess of the scope of Licensee's license, usage restrictions, or product limitations outlined in the applicable Agreement.