# Pega Cloud Acceptable Use Policy

## Additional Rights and Responsibilities

### During the term of the Subscription Services, Client will:

- Be responsible for the accuracy, integrity and legality of content and data;
- Be responsible for configuring a Guardrail Compliant Client Application and for the performance of such Client Applications;
- Be responsible for any third-party software, tool, library or component that is installed and/or used by or on behalf of the Client in any Environment in connection with the Subscription Services;
- Not use protected classes of data (such as protected health information, personally identifiable data, or other non-public client information) in a non-Production Environment;
- Not include Protected Health Information in a Production Environment unless using Pega Cloud HIPAA/HITECH Edition;
- Not include personally-identifiable data in a Production Environment unless identified in the Schedule to the Agreement;
- Not include confidential or sensitive data in the Client Application log files;
- Create and protect security credentials related to Client's use of the Subscription Services;
- Notify Pega within twenty-four (24) hours if it becomes aware of any actual or alleged data security incident at the application layer;
- Be responsible for third party data flows that the Client integrates with and into the Environments;
- Grant to Pega a worldwide, limited-term license to host, copy, execute, transmit and display Client's data, Client Applications and any Third Party Products, as necessary to provide the Subscription Services;
- Allow Pega to use anonymized information about Client's Subscription Services to upgrade and improve the Pega Cloud services.

### During the term of the Subscription Services Pega will:

- Not acquire any right, title or interest from Client in or to Client's data or any Third Party Products.

- Upon request and not more than once annually, deliver to Client (i) the current SSAE 18 SOC II Type 2 report, (ii) the current HIPAA/HITECH compliance opinion letter, (iii) the

current PCI-DSS Attestation of Compliance, (iv) the current penetration testing report, (v) an executive summary of Pega' Written Information Security Program and (vi) executive summaries of the security, data backup, and monitoring events for the Client's Environment(s) that are currently available.

- Notify Client without undue delay if it becomes aware of any actual security incident involving client data at the infrastructure layer, including a notification of loss affecting the confidentiality, integrity, or availability of Client data whether or not such data has been encrypted. In the event of such data breach, Pega will cooperate with Client in any manner reasonably requested by Client and in accordance with applicable law and regulations, including conducting the investigation, cooperating with authorities, and notifying affected persons and other appropriate entities.

- Upon request made within 15 days from termination of the Subscription Services, provide Client's data in a Production Environment database backup file encrypted to customary standards. Pega may delete any Client data once provided to Client or that is not requested within 15 days from termination of the Subscription Services, unless legally prohibited.