ACQUIA SECURITY ANNEX

A. Security of Data Processing

Acquia has implemented and will maintain technical and organisational measures inclusive of administrative, technical and physical safeguards to ensure a level of security appropriate to the risk of the data processing for the Acquia Services as described in this Acquia Security Annex (the "Security Measures"). These Security Measures may be changed by Acquia from time to time during the Term of the Agreement in order to take into account advancements in available security technologies. However, Acquia will not materially decrease the overall security of the Services during the Term of the Agreement.

This Acquia Security Annex supplements (1) the Acquia Subscription and Services Agreement available at http://www.acquia.com/downloads/ssa or the agreement existing between the parties (the "Agreement"), and (2) the Acquia GDPR Data Processing Addendum (the "DPA"). In case of a conflict between this Acquia Security Annex and the Agreement or DPA, the Agreement or the DPA shall prevail.

The Security Measures include, but will not be limited to, the following measures for ensuring the ongoing confidentiality, integrity and availability of Customer Data in order to prevent unauthorized access, use, modification or disclosure of Customer Data:

a) performance of background checks on all personnel, as well as signature of non-disclosure commitments and business ethics prior to employment;
b) security and privacy awareness training, inclusive of acknowledgment and agreement to abide by organizational security policies, for all personnel upon hire and annually thereafter;
c) pseudonymisation or encryption of Customer Data in transit and at rest utilizing industry-standard mechanisms for certain Acquia Services;
d) the ability to restore the availability and access to Customer Data in a timely manner in the event of an incident impacting the availability of Customer Data by maintaining a backup solution for disaster recovery purposes;
e) logging and monitoring of security logs via a Security Incident Event Management ("SIEM") system and alerting to a dedicated Incident Response team upon the detection of suspicious system and/or user behaviors;
f) processes and tooling for regularly identifying, assessing and triaging vulnerabilities based on industry-standard guidelines;
g) maintenance of a comprehensive set of security and privacy policies, procedures and plans that are reviewed on at least an annual basis and provide guidance to the organization regarding security and privacy practices;
h) processes for evaluating prospective and existing subprocessors to ensure that they have the ability and commit to appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity and availability of Customer Data; and,
i) a process for regularly testing, assessing and evaluating the effectiveness of administrative, technical and physical safeguards for ensuring the security of the processing, transmission or storage of Customer Data through external and internal audits as further described in Section C below;
j) preventing access, use, modification or disclosure of Customer Data except by authorized Acquia personnel (1) to provide the Subscription Services and prevent or address service or technical problems, (2) as compelled by law, or (3) as Customer expressly permits in writing.

By implementing the Security Measures detailed above Acquia takes into account the risks that are related to data processing, in particular the ones resulting from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

B. Acquia Shared Responsibility Model

Acquia Responsibilities
Acquia is responsible for the confidentiality, integrity and availability (the "security") of the Services and internal Acquia information technology systems. In addition to those measures detailed in "Security of Data Processing" above, Security Measures include, but are not limited to, server-level patching, vulnerability management, penetration testing, security event logging & monitoring, incident management, operational monitoring, 24/7 support, and ensuring customer site availability in accordance with SLA's.

Acquia uses Sub-processors for the Services and to support Acquia as a Processor of Customer data, all as more fully set forth on the website https://www.acquia.com/about-us/legal/subprocessors. As these Sub-processors are Authorized Contractors as defined in the Agreement, Acquia shall remain fully liable for their acts and omissions relating to the performance of the respective Services and shall be responsible for ensuring that obligations under this Security Annex and the Agreement are carried out in accordance with both.

Customer Responsibilities
The Customer is responsible for the security of their Customer Application(s), for example the open source software Drupal, that are used in conjunction with the Services. This includes, but is not limited to, ensuring a secure configuration and coding of the applications, related application security monitoring activities, Customer user access management, password configurations, implementing multi-factor authentication, periodic penetration testing, appropriate Application-level DoS or DDoS protections, and/or vulnerability scanning of their applications, amongst others.

In addition, Customers are also responsible for the secure management of their users that they manage and provision for the purpose of granting access to Acquia's Services and abiding by the Agreement, the DPA and Acquia's Acceptable Use Policy in using Acquia's Services.

C. Third Party Audits, Certifications

The Security Measures for Acquia's platform offerings, including ACE and ACSF, are subject to periodic testing by independent third party audit organizations, inclusive of the following audits and certifications:

- SOC 1 and 2
- PCI-DSS
- ISO 27001
- FedRAMP

Acquia will provide copies of current published audit reports for the Services to Customers upon written request and under NDA. Such audit reports, and the information they contain, are Acquia Confidential Information and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to the Services and are provided without any warranty.

D. Customer Audits

Acquia offers its Services in the cloud using AWS and a one-to-many business model that relies on standardization of best practices and industry standards for the benefit of its Customers. As a result, onsite audits by Customers pose security and privacy risks to Acquia, other Acquia Customers and Acquia Subprocessors. Moreover, AWS does not allow for physical audits of the AWS data centers but instead provides third party audits and certifications. It is for these reasons, among others, that Acquia's security program consists of the audits, certifications and available documentation detailed in "Third Party Audits, Certifications" above as part of balancing transparency regarding the security and privacy safeguards that Acquia has implemented, while also satisfying security and privacy requirements as part of security and privacy obligations to Acquia Customers, and its Sub-processors, including AWS.

Therefore, Customer agrees to exercise its right to conduct an audit or inspection of Acquia's processing of personal data within Customer Data by instructing Acquia to carry out the audits as described above in the section "Third Party Audits, Certification" using its current processes and timing. If Customer wishes to change this instruction regarding the audit or inspection, then Customer shall send such request by written notice to Acquia and the parties agree to jointly discuss how to implement the changed instruction.