ACQUIA SECURITY ANNEX

This Acquia Security Annex supplements (1) the Acquia Subscription and Services Agreement or the agreement existing between the parties (the "Agreement"), and (2) if applicable, the Acquia GDPR Data Processing Addendum (the "DPA"). Defined terms not otherwise defined herein shall have the means ascribed to them in the Agreement or DPA. In case of a conflict between this Acquia Security Annex and the Agreement or DPA, the Agreement or the DPA shall prevail.

1. Security Policy. Acquia maintains a company-wide information security management system and control program that includes written security policies, standards and procedures based upon ISO/IEC 27001:2013 (collectively, the "Acquia Information Security Policy"). The Acquia Information Security Policy requires:

a. the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Customer Data to the extent that such Customer Data is provided to Acquia and maintained or processed by Acquia during its provision of Services by utilizing practices such as:

   i. Secure software development practices;
   ii. Secure operating procedures and vulnerability management;
   iii. Ongoing employee training;
   iv. Controlling physical and electronic access to Customer Data, and
   v. Means for detecting and preventing intrusions and security system failures on critical systems.

b. that Acquia follow the principle of least privilege access, allowing only active Acquia employees and contractors access to records containing Customer Data and limits access to those persons who are reasonably required to know such information in order to accomplish a valid business purpose or to comply with record retention regulations;

c. that Customer Data that is identified as such to Acquia by the customer at intake, is secured appropriately commensurate to the nature of Customer Data, including any individual personal data provided to Acquia by Customer as set forth in this Exhibit, using commercially available and industry accepted controls and precautionary measures;

d. that commercially reasonable standards are followed with respect to strong change-control procedures and technical controls that enforce segregation of duties, minimum necessary dataset, and access controls;

e. monitoring of operations and maintaining procedures to ensure that security policies are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Customer Data, and continuously improving information safeguards as necessary to mitigate risks;

f. a security patch and vulnerability management process based on accepted industry standard practices and protocols, including, monitoring threats, and responding to vulnerabilities reported by third parties; and

g. A security incident response and disaster recovery planning, including documentation of responsive actions taken in connection with any security incident related to Customer Data.

2. Security Practices and Processes

a. Customers are responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored or transmitted through the Subscription Services for which regulations other than those set forth in the Security Annex apply. If, in the course of providing Subscription Services, Acquia agrees in writing to process such Customer Data and Customer has subscribed to any applicable Subscription Services, Acquia shall process it only as permitted under this Agreement and in compliance with data protection legislation to which Acquia is subject as a service provider. In the event that Acquia agrees to receive Customer Data from Customer, Acquia will manage and/or process such Customer Data pursuant to the security requirements, obligations, specifications and event reporting procedures as set forth in this Annex and the Agreement, and any amendments.

b. Acquia will comply with: (i) secure software development practices consistent with industry accepted standards and practices, and (ii) industry best practices on privacy and security.

c. Acquia restricts access to Customer Data and systems by users, applications and other systems. These controls include (i) controls to systems and data, limited to properly authenticated and authorized individuals based on principles of least privilege and need-to-know; and (ii) physical access controls, as described below. Acquia will limit access to Customer Data to the minimum necessary dataset required to accomplish the intended business purpose or use.

d. Acquia facilities and/or any Authroized Contractor facilities that process Customer Data will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., electronic locks, access badges, and video surveillance) that provide a physically secure environment.

e. Acquia logs access to controlled systems and records, including successful and failed system access attempts, and restricts, and restricts the connection times of users. Acquia will use unique logins on all network equipment, whenever commercially reasonable.

f. Acquia maintains processes to identify and deploy security patches in a timely manner. Unless otherwise expressly agreed in writing, "timely" means that Acquia will introduce a fix or patch as soon as commercially reasonable after Acquia becomes aware of the security problem or availability of a fix or patch.

3. Patch and Vulnerability Management.

a. Acquia follows commercially reasonable best practices for patch management, criticality ranking and patching time frame requirements for all Acquia-operated systems, switches, routers, appliances, servers, and workstation PC's, as applicable.

b. Where feasible, Acquia ensures that trusted, commercially available anti-virus software is installed, enabled, and kept current on Acquia servers and systems used in accessing, processing, transmitting, or storing Customer Data.

c. Acquia maintains trusted, current, commercially available anti-malware protection capabilities on Acquia devices, particularly those used for accessing, processing, transmitting, or storing Customer Data.

d. Acquia maintains a vulnerability management solution for devices connected to Acquia's LAN. Such solution is designed to regularly assess Acquia's network for known vulnerabilities.

4. Security Monitoring

a. Acquia has a designated security team which monitors Acquia's control environment which is designed to prevent unauthorized access to or modification of Acquia's Customer Data. Acquia regularly monitors controls of critical systems, network and procedures to validate proper implementation and effectiveness in addressing the threats, vulnerabilities and risks identified. This monitoring is variable by the criticality, exposure, and the system's assets and may include: (i) internal risk assessments; (ii) validation of Multi-Factor Authentication for select environments; (iii) third party compliance, including hosting services and third party components; and (iv) assessing changes affecting systems processing authentications, authorizations, and auditing.

b. Acquia performs periodic vulnerability assessments on Acquia applications and systems. Penetration tests are performed either by Acquia or by an established, reputable independent third party.

5. Security of Data Processing. Acquia has implemented and will maintain technical and organizational 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.

The Security Measures may 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. Background Checks

Performance of background checks on all personnel, as well as execution of non-disclosure commitments prior to employment and acknowledgment of professional behavior in the workplace documents, which includes anti-harassment and business ethics;

b. Training

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. Customer Data

Pseudonymisation or encryption of Customer Data in transit and at rest utilizing industry-standard mechanisms for certain Acquia Services;

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 below;

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.

d. Availability

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

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. Vulnerability Triaging

Processes and tooling for regularly identifying, assessing and triaging vulnerabilities based on industry-standard guidelines;

g. Policies

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; and,

h. Subprocessors

Processes for evaluating prospective and existing Subprocessors to ensure that they have the ability and commit to appropriate administrative, technical and physical measures to ensure the ongoing confidentiality, integrity and availability of Customer Data.

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, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

6. Secure Data Transmissions. Any Customer Customer Data that Acquia transmits over a public communications network will be protected during transmission by using, or making available, industry accepted standards such as TLS, SSH and VPNs.

7. Data and Media Disposal. Acquia maintains procedures that align with industry standards, such as NIST SP 800-88, regarding the disposal of both tangible property and electronic files containing Customer Data, taking into account available technology so that Customer Data cannot be reconstructed and read.

8. Backup and Retention. Acquia will backup systems used to provide services to Customer to ensure adequate recovery capabilities in accordance with the schedule set forth in the Documentation for the applicable Services. Back-ups will be appropriately protected to ensure only authorized individuals are able to access the Customer Data, including but not limited to encryption of data stored off-site in electronic media and appropriate classification and protection of hard copy records, as applicable. If not separately backed up, Acquia will secure any files containing Customer Data against unauthorized access in accordance with the terms of the Agreement.

9. Customer Data. Acquia will comply with applicable laws and regulations to the provision of the Services concerning the confidentiality, security, and processing of any Customer Data that it receives from Customer. In the event Acquia processes types of Customer Data that are subject to additional regulatory requirements due to the nature of the data or its place of origin (as defined in section 2a above) Acquia will reasonably cooperate with Customer to arrange compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., EU Standard Contractual Clauses, Business Associate Agreement governing Protected Health Information), implementation of additional security controls required by relevant law, completion of regulatory filings applicable to Acquia, and participation in relevant regulatory audits as applicable from section 13 below.

10. Security Incident Management and Remediation. For purposes of this Annex, a "**Security Incident**" means (i) the loss of, (ii) unauthorized acquisition, use or disclosure of, or (iii) unauthorized access to, Customer Data resulting from a security breach of the Acquia platform. Acquia maintains a response function capable of identifying and assessing the seriousness and extent of a Security

Incident, mitigating the effect of a Security Incident, conducting root cause analysis, implementing and documenting remedial action plans, and preventing the recurrence of Security Incidents. Acquia has an established set of procedures to ensure personnel and contractors promptly report actual and/or suspected breaches of security. Acquia keeps an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents, as well as performing required recovery actions to remedy the impact.

a. Security Incidents on Acquia's platform are logged and reviewed, secured, and retained as required by applicable laws and regulations.

b. In the case of a Security Incident that relates to Customer Data, Acquia shall (a) promptly assess and contain such Security Incident, (b) notify Customer, without undue delay, upon becoming aware of such Incident, and in no case later than forty-eight (48) hours after Acquia has become aware of such Security Incident, via a Support ticket to each of the individuals identified by Customer for distribution of such Support Tickets (or such other addresses as may be provided by Customer from time to time) and provide regular status updates to Customer regarding the investigation at a frequency reasonably requested by Customer depending upon the severity of such Incident, (c) as applicable, provide reasonable cooperation and assistance to Customer needed to fulfill Customer's obligations related to Customer's use of the Services, as applicable, and (d) immediately take all steps reasonably necessary and within Acquia's reasonable control, including without limitation, those reasonably requested by Customer, to limit, stop, prevent and remediate such Incident. Following this initial notification, Acquia will promptly investigate the Security Incident and take all reasonable and necessary steps to prevent any further compromise of the Customer Data. If a security deficiency is identified within any Acquia information system during this investigation, Acquia will provide a report to Customer containing a description of the nature of the Security Incident, an identification of any Customer Data that was disclosed, destroyed, altered or compromised, and any investigative, corrective, or remedial actions taken or planned by Acquia to mitigate the risk of further Security Incidents. Acquia will maintain log files sufficient to enable Customer to determine what Customer Data was accessed and when, regardless of whether such data is physically or electronically maintained.

11. Business Continuity and Disaster Recovery. Acquia maintains business continuity and disaster recovery planning processes to establish and maintain plans and procedures for the continuity, recovery and operation of information systems, processes and facilities that could impact the availability of Customer Data (**"BC/DR Plans**"). These BC/DR Plans include processes for responding to emergencies (e.g., natural disasters such as fire, earthquakes, or hurricanes, or other disasters such as sabotage, virus, and terrorism), and includes: (i) descriptions of roles and responsibilities: identifying key individuals and the recovery team responsible for implementing recovery actions; (ii) data backup plans, providing for periodic backups of data from database systems that can be used to reconstruct data; (iii) contingency plans and disaster recovery guides that will be followed by members of the recovery team before, during and after an unplanned disruptive event in order to minimize downtime and data loss; and (iv) procedures for annual testing and evaluating the BC/DR Plans including documenting the tests in writing.

12. Security Evaluations.

a. Acquia performs periodic risk assessments that evaluate and assess the security of the system's physical configuration and environment, software, information handling processes, and user practices including appropriate logs and reports on security activity.

b. In addition, security policies are regularly reviewed and evaluated to ensure operational effectiveness, compliance with applicable laws and regulations, and to address new threats and risks.

c. Security Policies are also reviewed when there is a material change in Acquia's business practices or the external threat environment that may reasonably implicate the security or integrity of records containing Customer Data. Acquia uses a documented change control process for software, systems, applications, and databases that ensures access changes are controlled, approved, and recorded.

d. Acquia will promptly notify Customer of any planned system configuration changes or other changes that would adversely affect the confidentiality, integrity, or availability of Customer's Customer Data.

13. Acquia Certifications and Standards by Product Offering

Acquia engages reputable third-party, independent, audit firms to conduct the below audit engagements:

Acquia Offering	Completed Certifications and Attestations
Acquia Cloud Enterprise	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • HIPAA[1] • PCI-DSS[2] • FedRAMP[3]
Acquia Cloud Site Factory	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • HIPAA[1] • PCI-DSS[2] • FedRAMP[3]

[1] HIPAA compliant indicates that the service can be used in a way that enables Customers to help meet its legal obligations for HIPAA compliance. Ultimately, Customers are responsible for ensuring compliance with legal obligations, that the Acquia service meets their compliance requirements, and that they secure the service appropriately. Customers can reference Acquia's SOC 2 report, which contains a matrix mapping HIPAA controls to Acquia's SOC 2 controls.

[2] PCI-DSS compliance requires the purchase of Acquia's PCI Cloud configuration within Acquia Cloud Enterprise and Acquia Cloud Site Factory.

[3] Federal Risk and Authorization Management Program ("FedRAMP") is available for select Customers (i.e. Federal Agency cloud deployments). Acquia's FedRAMP implementation is more fully described in its FedRAMP package, available via the OMB MAX repository system.

Acquia will provide copies of available audit reports for the applicable 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. Acquia can also provide summary level penetration test documentation available to Customers upon request sanitized of any sensitive information.

14. Training and Secure Development Practices. The Acquia Information Security Policy is communicated to all Acquia personnel, employees, and contractors. Acquia provides periodic and mandatory security awareness training to employees and contractors (collectively "Personnel"). Acquia imposes disciplinary measures for violations of the Acquia Information Security Policy:

a. Agreements with relevant subprocessors include requirements that these subprocessors address security risks, controls, and procedures for information systems and contain terms, conditions, and restrictions at least as protective and as restrictive as those set forth herein. Acquia shall supply each of its personnel and contractors with appropriate, ongoing training regarding information security procedures, risks, and threats and Acquia shall be responsible for the performance of any subcontractor. Acquia agrees that any Services performed for Customer involving use of Customer Data shall be performed only at the Data Center Region and by personnel permitted under the Agreement.

15. 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 the applicable SLA.

Acquia uses subprocessors for the Services and to support Acquia as a Processor of Customer data, all as more fully set forth on the website located at: https://www.acquia.com/about-us/legal/subprocessors. As these subprocessors are authorized subprocessors 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), as applicable. For example patching 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 and provision of users for the purpose of granting access to Acquia's Services and abiding by the Subscription and Services Agreement, the Data Processing Agreement and Acquia's Acceptable Use Policy in using Acquia's Services.

16. Access and Review. Acquia will make summary level information regarding its security policies and procedures as well current, published, third-party audit audit reporting related to Customer's Customer Data available for Customer's review at Acquia upon reasonable prior written notice by Customer and subject to Acquia's confidentiality and security conditions, and subject to a written and mutually agreed audit plan. Acquia reserves the right to require its prior approval to any third party review of the DR Plan, and reasonably condition and restrict such third party access. As illustrated in, "Acquia Certifications and Standards by Product Offering" Customers may also review available audit reporting as outlined in Section 13.

17. 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 Subprocessors, 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 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.

Disclaimer: Information in this document is subject to change without notice. For more information on Acquia solutions and controls, please contact Acquia. Further detail on Acquias offerings, including SLAs and physical, administrative and technical safeguards are available.