# TAULIA PLATFORM DATA SECURITY STANDARD POLICY

## 1. Definitions

"**Affiliate**" means any legal entity in which Taulia or Customer, directly or indirectly, holds more than 50% of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.

"**Agreement**" means an "Agreement" as described in an Order Form

"**Business Partner**" has the meaning stated in the General Terms and Conditions for Cloud Services attached to an Order Form.

'**Cloud Service**" means a "Cloud Service" as selected by a Customer in an Order Form.

"**Confidential Information**" means all information which the disclosing party protects against unrestricted disclosure to others that the disclosing party or its representatives designates as confidential, internal and/or proprietary at the time of disclosure, should reasonably be understood to be confidential at the time of disclosure given the nature of the information and the circumstances surrounding its disclosure.

"**Customer**" means an entity named as "Customer" on an Order Form

"**Customer Data"** means any content, materials, data and information entered by any person into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include Taulia's Confidential Information and for the avoidance of doubt excludes any content, materials, data and information entered by any person in any environment for the purpose of testing or demonstration.

"**Taulia**" means Taulia LLC or its Affiliates.

## 2. Security Controls.

Taulia shall implement and maintain current, industry standard security procedures, practices and controls commensurate to assure that all Customer Data and any information provided by Business Partners, are only accessed by Taulia's authorized personnel and subcontractors, Customer, its Affiliates, and the Business Partner that Customer specified as recipient of such data, and to safeguard against unauthorized access, destruction, use, alteration or disclosure of any such data and information. Security controls and safeguards shall include, without limitation, restriction of physical access to such data and information, implementation of logical access controls, encryption of data, sanitization or destruction of media, including hard drives, and establishment of an information security program that at all times is at least as stringent as documented and audited in Taulia's most recent SOC 1 Type II / SSAE18 or SOC 2 Report, as applicable and available. In addition, Taulia and its subcontractors shall update their respective security procedures, practices, policies and controls so as to keep current with industry standards. Taulia currently uses Amazon Web Services (AWS) and Google Cloud Platform (GCP) for its data centers, which Customer deems in compliance with its security requirements. AWS and GCP data centers are, and any other data center Taulia may in the future use in production to collect, receive and/or store Customer Data shall be data centers that satisfy the standards for a Tier 3 data center facility. Taulia shall (unless prohibited by applicable law or regulation) promptly report any unauthorized access or disclosure of Customer Data to Customer and shall take all reasonable measures within its control to immediately stop the access or disclosure and prevent recurrences.

## 3. Encryption of Your Data at Rest.

Taulia and its subcontractors (as applicable) shall use industry best practices to implement security procedures which will encrypt the following information: i) bank details, ii) tax identifiers and iii) PO line item descriptions. Taulia may decide to encrypt further data at rest entirely at its discretion.

## 4. SOC 1 Type II / SSAE 18 or SOC 2 Reports.

Taulia represents that all production servers that will receive, process and store Customer Data will be located in a SOC 1 Type II / SSAE 18 or SOC 2 certified facility maintained by Taulia or a subcontractor (collectively, “Server Facility”). During the term of this Agreement, Taulia will ensure that Taulia and its subcontractors’ Server Facilities undergo SOC 1 Type II / SSAE 18 or SOC 2 review, as applicable, on an annual basis.

At least annually, Taulia and its applicable subcontractors shall assist Customer in obtaining a copy of the then-current SOC 1 Type II / SSAE 18 or SOC 2 Report from Taulia, as applicable and available, as well as from the owner or operator of the Server Facility where Customer Data is saved and/or stored (at no cost to Customer) as well as a copy of any other report that documents Taulia is meeting the security requirements set forth herein. Customer agrees that in order to view these reports, it may be required to sign a Non-Disclosure Agreement with the entity whose Server Facility is the subject of the report.