

## **Security Measures for Cloud Services (“Security Measures”)**

These Security Measures complement the Technical and Organizational Measures referenced in the DPA and define the current technical and organizational measures maintained by Taulia to protect Customer Data. Taulia may change the Security Measures at any time without notice, provided Taulia maintains a comparable or better security level. Individual measures may be replaced by new measures that serve the same purpose without diminishing the overall security level protecting Customer Data.

### **1. INFORMATION SECURITY GOVERNANCE**

**1.1. Security Framework.** Taulia maintains a formal security framework with written policies and standards designed to protect the confidentiality, integrity, and availability of Customer Data (“Taulia Security Framework”). The Taulia Security Framework: (i) is approved by Taulia management; (ii) supports the measures described in the Security Measures; and (iii) is reviewed at least annually by Taulia stakeholders to assess opportunities for improvement, changes in technology, and risks.

As part of this stakeholder review, Taulia considers guidance from independent third-party sources such as the National Institute of Standards and Technology (NIST), British Standards Institute (BSI), and the International Organization for Standardization (ISO).

**1.2. Executive Oversight.** Taulia maintains a Chief Security Officer (or an equivalent executive) responsible for overseeing the Taulia Security Framework and communicating essential security topics to the Taulia Board of Directors.

### **2. SECURITY CERTIFICATIONS & ATTESTATIONS**

**2.1. Internal Assessment.** Taulia regularly assesses the effectiveness of security controls within the Taulia Security Framework.

**2.2. Independent Third-Party Review.** Taulia conducts certain external audits with third-party auditors to provide independent security assurances.

**2.3. Self-Service Reviews.** Taulia obtains certain third-party certifications and attestations. Customer may conduct self-service reviews of obtained security certifications and attestations for a subscribed Cloud Service as Taulia is permitted to make available to customers of the Cloud Service (e.g., ISO 27001, SOC 2, or other comparable reports). Customers may request available certifications and reports on the Taulia website.

### **3. ORGANIZATIONAL SECURITY MEASURES**

**3.1. Limited Use of Customer Data.** Taulia processes Customer Data only in accordance with the Agreement including the applicable confidentiality and nondisclosure obligations.

**3.2. Security Risk Management.** Taulia maintains a risk management program designed to identify, analyze, and manage threats to the Cloud Service.

#### **3.3. Human Resource Security.**

**3.3.1.** Before granting access to Customer Data, Taulia: (i) performs a pre-employment screening on employees unless restricted by law; (ii) enters into a confidentiality agreement with employees; and (iii) mandates employee training on information security.

**3.3.2.** Taulia maintains a Global Code of Ethics and Business Conduct (“Code of Conduct”) outlining SAP’s and Taulia’s values and standards for ethical business. Taulia mandates employees to adhere to the Code of Conduct, and Taulia internally investigates suspected breaches of the Code of Conduct.

**3.3.3.** Employees complete role-based security and privacy training, acknowledge communication of written security policies, and receive regular awareness education.

**3.4. Asset Management.** As part of Taulia’s internal asset management process, Taulia is responsible for: (i) inventorying assets; (ii) assigning ownership; (iii) categorizing assets into defined written classes; (iv) tracking and monitoring assets; and (v) defining acceptable use of assets.

**3.5. Third-Party Risk Management.** Taulia maintains a third-party risk management program that manages supplier risks to the Cloud Service (“TPRM Program”). At minimum, the TPRM Program includes: (i) established third-party engagement policies; (ii) risk assessments; and (iii) controls and processes to monitor contract compliance between Taulia and its third-party suppliers.

**3.6. Secure Cloud Development.** Taulia maintains a secure development and operations lifecycle framework designed to mitigate software development risks to the Cloud Service (“SDOL Framework”). At minimum, the SDOL Framework is designed to: (i) define criteria for software security assessments and releases; (ii) protect code from unauthorized access and tampering; (iii) verify and test software release integrity; and (iv) identify and manage known vulnerabilities.

**3.7. Change Management.** As part of the broader Taulia Security Framework, Taulia maintains formal change management processes (“Change Management”). At minimum, Change Management requires that material changes to the Cloud Service are planned, tested, and approved.

## **4. PHYSICAL SECURITY MEASURES**

**4.1. Data Center Measures.** Data centers are protected using multiple measures designed to prevent unauthorized individuals from gaining physical access to data centers hosting Customer Data. These physical access measures include key/access systems, security zones, access credentials, door locks, guards, cameras, motion sensors, alarm systems, and other applicable measures designed to protect equipment and facilities from compromise. To protect proper functionality, physical security equipment undergoes regular maintenance and security checks, and is supported by uninterrupted power supplies (e.g., UPS, batteries, generators, etc.).

**4.2. Personnel Access.** Access rights are granted to authorized persons on an individual basis in accordance with written policies (see access control details below). Only authorized persons with appropriate credentials have access to systems and infrastructure within data centers hosting Customer Data. Guests and visitors must register and log their names and times at reception upon entry.

**4.3. Physical Media Disposal.** Physical media is disposed in accordance with physical decommissioning policies. Before disposing physical media, commercially reasonable erasure methods render Customer Data on physical media unrecoverable.

## **5. TECHNICAL SECURITY MEASURES**

**5.1. Security Logging and Monitoring.** Cloud Service monitoring is designed to check the ongoing confidentiality, integrity, and availability of the Cloud Service, which includes logging information system and infrastructure events. Logged activities from network devices and systems are fed into Taulia’s Security Information and Event Management (SIEM) system(s), or similar central monitoring system(s), which generate appropriate alerts.

**5.2. Intrusion Monitoring.** Taulia uses intrusion detection mechanisms to monitor the Cloud Service for unauthorized intrusions.

**5.3. System Hardening.** Taulia maintains system hardening policies and processes to promote the security of the Cloud Service.

**5.4. Data Integrity.** Taulia deploys a multi-layered defense strategy that protects against unauthorized modifications of Customer Data. Customer Data may only be read, copied, modified, or removed by Taulia in accordance with the Agreement.

**5.5. Secure Data Deletion.** Taulia securely deletes Customer Data in accordance with the Agreement.

**5.6. Data Segregation.** Taulia employs various methods designed to segregate Customer Data from data of other Taulia customers including: (i) physical designs; (ii) logical designs; and (iii) server, operating system, and database restrictions.

## **5.7. Access Control.**

**5.7.1. Access Management.** Access controls provide identity management and grant appropriate access rights (“Access Management Controls”). Access Management Controls are designed to follow the principles of “least privilege,” “need-to-know,” and “segregation of duties.”

**5.7.2. Personnel Access.** Taulia personnel are issued a unique identifier to access Taulia’s systems. Taulia maintains written procedures to administer access authorization changes and access rights are revoked when personnel are no longer authorized to access applicable systems (e.g., termination of employment).

**5.7.3. Administrative Rights.** Administrative rights are only assigned to privileged and technical Taulia users on a “least privilege” and “need-to-know” basis.

**5.7.4. Password Management.** Taulia maintains a written password management policy that defines minimum requirements such as length, complexity, expiration, and lockout requirements.

**5.8. Secure Data Transmission.** Taulia secures the exchange or transmission of Customer Data between Taulia systems that constitute the Cloud Service. Measures for securing the exchange of information may include email encryption, provisioning of secure network protocols and interfaces, or features and functionality that support “data in transit” encryption (e.g., communication encryption protocols, server-to-server authentication, certificate authentication). Customer assumes responsibility for any data transfer once it is outside of Taulia-controlled systems (e.g., data being transmitted outside the firewall of the Taulia data center). Taulia recommends that Customer enables encryption of Customer Data in transit between Customer’s network and the Cloud Service to protect against unintended disclosure or modification of Customer Data where applicable.

**5.9. Secure Data Storage.** Customer Data is encrypted at rest while stored in the Cloud Service.

**5.10. Malware Management.** Taulia uses up-to-date anti-malware software designed to protect Customer Data from malware that may negatively impact the confidentiality, integrity, or availability of Customer Data.

**5.11. Endpoint Devices.** Taulia maintains security mechanisms on its devices that access Customer Data. Mechanisms may include firewalls, anti-malware software, disk encryption, restrictions to limit disablement of security mechanisms, and default systems for timeout locks. Taulia maintains a list of prohibited software that may not be installed on Taulia devices.

**5.12. Vulnerability and Patch Management.** Taulia maintains processes to monitor, detect, and respond to security vulnerabilities. At minimum, these processes require: (i) periodically reviewing third-party vulnerability alert services and official public disclosures posted on software vendor websites relevant to the Cloud Service; (ii) establishing internal vulnerability evaluation criteria; (iii) periodically conducting vulnerability scans; and (iv) patching the Cloud Service in accordance with operational procedures.

**5.13. Penetration Testing.** Taulia will conduct penetration testing and maintain internal policies that govern how the Cloud Service is proactively tested.

**5.14. Additional Details.** Customer may review additional technical details in each Cloud Service's respective Documentation.

## **6. RESILIENCY**

**6.1. Backups.** Taulia periodically backs up Customer Data and maintains alternative data centers to enable secondary storage of backup data. Backups are automated and the Cloud Service backup process includes hardware-independent restore and recovery capabilities. Taulia's backup and recovery process is tested regularly.

**6.2. Continuity and Recovery.** Taulia maintains disaster recovery or data resiliency procedures reasonably designed to safeguard the availability of the Cloud Service and Customer Data ("Resiliency Procedures"). At minimum, Resiliency Procedures include: (i) Customer Data backups (as described above); (ii) secondary storage locations; (iii) personnel with sufficient training to implement and support the Resiliency Procedures; (iv) testing or validating Resiliency Procedures at least once per calendar year; (v) maintaining written policies or standards that govern Resiliency Procedures; and (vi) crisis and process continuity plan(s) to protect operations during a major disruption event.

## **7. SECURITY INCIDENT MANAGEMENT**

**7.1. Security Incident Management Program.** Taulia maintains a security incident management program designed to detect, investigate, and respond to declared security incidents that impact the Cloud Service ("Incident Management Program"). At minimum, the Taulia Incident Management Program is: (i) approved by management; (ii) supported by teams with documented roles and responsibilities; and (iii) annually reviewed and tested.

**7.2. Security Incident Assessment Process.** As part of the Incident Management Program, Taulia maintains written policies and standards that govern how Taulia assesses and analyzes potential security incidents that may impact the Cloud Service ("Security Incident Assessment Process"). At minimum, the Security Incident Assessment Process is designed to do the following: (i) assess, classify, and prioritize security incidents in accordance with Taulia's written incident response plan; (ii) if appropriate, perform a security root cause analysis when Customer Data is impacted; and (iii) establish a process to attempt to reduce the likelihood of similar security incidents from impacting the Cloud Service in the future.

**7.3. Customer Notification.** Taulia will electronically notify Customer's registered contact(s) without undue delay after confirming a security breach has resulted in the unauthorized destruction, loss, alteration, or third-party access to Customer Data ("Customer Data Breach Notification"). As part of the Customer Data Breach Notification, Taulia will provide relevant and available information to Customer (e.g., material details, planned mitigation steps, and/or recommended Customer actions). Taulia's delivery of a Customer Data Breach Notification will not be construed as an acknowledgement or admission of any fault or liability.

## **8. REPORTING & UPDATES**

**8.1. Customer Event Reporting.** Security events can be reported through Taulia's customer support portal.

**8.2. Security Contacts.** Customer must register one or more security contacts within the support portal made available to Customer.

**8.3. Updates.** Taulia will publish updated versions of the Security Measures on its website and Customer may subscribe to receive automated notification (or other link provided by Taulia from time-to-time).

**8.4. Shared Responsibility.** Customer acknowledges that the Cloud Service makes certain security features available that Customer is responsible for enabling or otherwise configuring.