Acceptable Use Policy
For
Cloud Service Clients
Version 1.0

June 2020

Notice: This document represents Aptitude Software's current practices as of the date of issue of this document, which are subject to change without notice. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Aptitude Software, its affiliates, suppliers or licensors. The responsibilities and liabilities of Aptitude Software to its clients are controlled by Aptitude Software's agreements, and this document is not part of, nor does it modify, any agreement between Aptitude Software and its clients.

Document Control

(1) Document Description:

Aptitude Software Group Plc's (hence 'Aptitude Software' or 'Company') Acceptable Use Policy for Cloud Service Clients

(2) Document Location:

Prospective and current clients for Aptitude Software's Cloud Services can access to this policy at https://www.aptitudesoftware.com/security-trust-center/

(3) Document Revision History:

Revision Draft Date	Author	Version	Change Reference
6/15/2020	Chandra Kulkarni – Information Security Officer	Version 1.0	New Policy separately documents Acceptable Use requirements for cloud service users

(4) Document Approval History:

Approval Date	Approver	Version	Reference
6/18/2020 DocuSigned by: Chris Beed F5F002264FED4B5...	Chris Beed – Director of Information and Services	Version 1.0	Approved on behalf of the Information Security Committee

(5) Questions and Comments:

If you have further questions or would like additional information regarding Aptitude Software's Information Security Policy, please contact the following:

Information Security Officer (ISO) at information-security@aptitudesoftware.com

Acceptable Use Policy for Cloud Services

Aptitude Software Cloud Services

Aptitude Software provides products and services to clients (also referred to as 'system users', 'users' or 'user entities') through its cloud finance products portfolio and currently provides multiple financial management application deployments as cloud services. Such applications are delivered through a system of core product, service and supporting application elements referred to as the Aptitude Software Cloud Services system.

Typical elements of the system include

- Core financial transaction processing application software such as Aptitude Lease Accounting Engine (ALAE) or Aptitude RevStream (AREV)
- Application infrastructure elements including Amazon Web Services (AWS), database and server software and monitoring tools.
- Supporting services and tools including JIRA Service Desk which support the core application.
- Microsoft Teams or other video conferencing and networking tools

General Use Requirements

Users are required to ensure that use of the cloud services system meets the following requirements

- Users are responsible for exercising good judgment regarding appropriate use of cloud services resources in accordance with contractual requirements, internal standards, and guidelines. Aptitude Software Cloud Services resources may not be used for any unlawful or prohibited purpose.
- For security, compliance, performance, and maintenance purposes, Aptitude Software authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the Aptitude Software system may be disconnected. Users are required to provide responses to events or incidents identified in the context of such monitoring where user assistance is required.
- Aptitude Software Cloud Services systems are not designed to process or store client personal data, personal health data, export-controlled data[1] or payment card data. Users should ensure that the data processed by or stored in the system is consistent with the anticipated use of the system and are required to notify Aptitude Software in the event of any current or planned deviations.
- Users are required to notify and seek the prior written approval of Aptitude Software Information Security or Aptitude Software Client Support (information-security@aptitudesoftware.com) in advance of any potential or planned use of the cloud services system by third parties including auditors, penetration testers or other vendors who are not contracted directly with Aptitude Software.

Service Organization Controls (SOC) Reporting and System Use

- Aptitude Software will maintain SOC 1 Type II reports for its cloud services. In the first year of service operation, the reports will typically cover a period which is less than 12 months but no shorter than three months. On-going reports will cover a period of 12 months.

[1] Export Controlled Data – Client data which is subject to the Export Control Laws of the United States (Export Control Laws are federal laws implemented by the U.S Department of Commerce (Export Administration Regulations) and U.S Department of State (International Traffic in Arms Regulations))

- SOC2 Type II reports may be provided for certain cloud services where relevant in addition to SOC1 reports.

- Further details regarding Aptitude Software's SOC program may be obtained at the following location https://www.aptitudesoftware.com/security-trust-center/

- Clients and user entities are required to comply with complementary control requirements identified within the service specific SOC1 reports

Complimentary User Control Requirements

Aptitude Software Cloud Services systems are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. A detailed listing of the controls and the background and requirement for such controls is provided within Aptitude Software's Service Organization Controls (SOC) reports for the specific cloud service. The requirements include (but are not limited to the) controls to ensure the following:

- report any system issues to Aptitude Software.
- notify Aptitude Software with a request to perform client validation testing or User Acceptance Testing.
- notify Aptitude Software when client validation testing is complete, thus approving that the testing was completed successfully.
- approving changes to production for cloud clients.
- notify Aptitude Software with any issues found following upgrades and maintenance of the application.
- promoting change related to their own customizations and integration and keeping track of them.
- User entities are expected to implement controls that ensure that the necessary system and browser configurations are installed to allow users to access the application.
- administering, provisioning and de-provisioning, and periodic review of individual user access (including assigning user roles) relating to their application and the Aptitude Software VPN (if used).
- password policies, appropriate password management and parameters for the application are updated and in place (including for client SSO solutions utilized for authentication)
- maintaining the security and confidentiality of user IDs and passwords for the application.
- procedures in place to control access (for example user IDs and passwords) to personal computers (PCs) used to enter, transmit, and report the application information.
- notify Aptitude Software of any security breaches or events at information-security@aptitudesoftware.com.
- secure and monitor transmissions originating from user systems to Aptitude Software.
- secure the username and password used to transmit data to the application.
- maintain and retain necessary supporting documents and records for all data entered and processed within the application.
- maintain and monitor the data transmitted to Aptitude Software to ensure data is secured appropriately based on its sensitivity.
- review incident and service level reports provided by Aptitude Software, where applicable, and reporting any issues based on the terms of the service agreement.
- ensure backup and retention policies and schedules are appropriate for their needs.
- contact Aptitude Software through Aptitude Software Service Desk with restore requests, if applicable.
- identify a responsible point of contact to provide oversight to the engagement between Aptitude Software and the client.
- perform validation testing of changes before they are implemented into client production environments.
- implement controls that ensure that they control the information that is shared outside of their respective networks and systems.

Reseller and Managed Service Provider Use Requirements

Resellers and managed service providers are treated the same way as clients by Aptitude Software and any use requirements which apply to clients are also applicable to resellers and managed service providers.

The following additional use requirements also applicable:

- Resellers and other entities acting on behalf of end users ('resellers') will ensure that end user data is appropriately segregated by requesting separate set up during system implementation
- Managed service providers processing transactions on behalf of end clients will ensure the segregation, completeness and accuracy of transaction processing.
- Aptitude Software will not be responsible for intentional or accidental comingling or loss of end user entity data due to service provider or reseller actions.
- Resellers and managed service providers will ensure that they assess end user entity requirements including any Service Organization Controls (SOC) reporting required for them. Aptitude Software can only respond to and address service provider reporting requirements for entities which it is directly contracted with.
- Resellers and managed service providers access to Aptitude Software infrastructure components including databases and servers will be limited to the service role performed by the provider. Aptitude Software does not anticipate resellers and service providers requiring access to data storage systems to write or modify transaction data through the data access layer (back end) and any data changes to production systems should be initiated through the application presentation layer (front-end) or through a Aptitude Software Service Desk ticket only.
- Resellers will notify Aptitude Software regarding end user entity go-live or completion of implementation events in order to ensure that access to production systems is appropriately restricted.
- Resellers are responsible for ensuring that they provide support to end user entities they are contracted with. Aptitude Software will not maintain communications or services to third parties which are not a part of the contractual agreements.

Limitations on use

Clients may not

- release to any third party the results of any formal evaluation of the Service performed by or on behalf of Customer without the prior written approval of Aptitude Software, such approval not to be unreasonably withheld.
- license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit or make the Service available to any third party
- modify or make derivative works based upon the Service or reverse engineer the Service
- access the Service in order to build a competitive product or Service whether used internally or licensed to others
- use the service to send spam or otherwise duplicative or unsolicited messages in violation of applicable laws;
- send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children or violating third-party privacy rights;
- send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs
- interfere with or disrupt the integrity or performance of the Service or the data contained therein; or (v) attempt to gain unauthorized access to the Service or its related systems or networks.
- run system queries or transactions which impact the availability of the cloud services system.

Remote Collaboration and Conferencing Tools

Users must ensure that all usage of audio and video collaboration tools is in accordance with applicable privacy, personal data and social media policies. Aptitude Software professionals will avoid recording client personal videos during such interactions but are not responsible for any accidental or incidental recordings performed during the use of such tools for business purposes.

- Business video collaboration tools are installed on Aptitude Software PC's when required for business purposes, for example, for communicating with remote customers. Clients should notify Aptitude Software in the event they identify any concerns regarding the use of such tools.

- Aptitude Software professionals ensure that all business use of video collaboration tools is carried out with accounts created using their company email address as the account identity. Client users should ensure that they follow required security instructions for such interactions when using Aptitude Software remote interaction tools.

- Client hosted conferencing tools should specify shared conference passwords which must be specified for the session. Where possible, Aptitude Software personnel will use in-browser functionality rather than installing a specific application or program requested by the client. If the security of client hosted conferencing tools does not meet required standards, Aptitude Software may recommend alternative tools to protect the integrity and confidentiality of client data.

Malware Detection Events

- Clients should notify Aptitude Software in the event of any known malware attacks on client systems including those required to access Aptitude Software Cloud Services systems such as client end-user systems, laptops, client SSO solutions and applications for transferring data to and out of cloud services systems.

- Notification should be provided at information-security@aptitudesoftware.com

System Availability Events

- Clients should notify Aptitude Software in the event of any known client system outages including SSO systems which are utilized for authenticating to Aptitude Software Cloud Services systems. Clients are required to follow Aptitude Software instructions during such situations including use of third-party authentication systems for the timeframe of client system outage.

- Notification should be provided at information-security@aptitudesoftware.com

Acceptable Use Policy Enforcement

Aptitude Software will contact and notify the client in the event of violations of the Acceptable Use Policy. Continued violation post notification may result in suspension of access to the system. Aptitude Software also reserves the right to suspend or terminate access in the event such actions are required to protect the confidentiality, integrity and availability of cloud services data including data for other clients serviced by Aptitude Software.