



**Acceptable Use Policy  
For  
Aptitude Cloud  
Services**

**Version 2.0  
February 2024**

## **Aptitude Software Group Plc – Acceptable Use Policy for Cloud Service Clients**

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.

The information contained in this document is owned by and confidential to Aptitude Software Group Plc and members of its group companies (together “Aptitude Software”) and must not, therefore, be disclosed to any third party without the express written permission of Aptitude Software. Information in this document is subject to change without notice and does not represent a commitment on the part of Aptitude Software. In addition, no part of this document may be reproduced or transmitted in any form or by any means electronic or mechanical including photocopying, recording or information storage and retrieval systems, for any purpose other than the recipient’s personal use without the express written permission of Aptitude Software.

## Aptitude Software Group Plc – Acceptable Use Policy for Cloud Service 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.apitudesoftware.com/security-trust-center/>

#### (3) Document Revision History:

Date	Author	Version	Change Reference
6/15/2020	Chandra Kulkarni – Information Security Officer	Version 1.0	<ul style="list-style-type: none"> <li>New Policy separately documents Acceptable User requirements for cloud service users</li> </ul>
6/28/2021	Chandra Kulkarni – Information Security Officer	Version 1.1	<ul style="list-style-type: none"> <li>Section Title change from 'Reseller and Managed Service Provider Use Requirements' to 'Third Party Use Requirements'</li> <li>Minor changes to Third Party Use Requirements section.</li> </ul>
5/16/2022	Chandra Kulkarni -Information Security Officer	Version 1.2	<ul style="list-style-type: none"> <li>Incorporating changes to accommodate for MPP acquisition</li> <li>Incorporating changes to accommodate for Fynapse (new product launch)</li> </ul>
8/09/2023	Chandra Kulkarni – Information Security Officer	Version 1.3	<ul style="list-style-type: none"> <li>Change in branding to reflect new logo</li> <li>Adding new section on use of client data</li> <li>Reflect changes specific to eSuite Cloud Service</li> </ul>
2/6/2024	Chandra Kulkarni – Information Security Officer	Version 1.4	<ul style="list-style-type: none"> <li>Minor changes to client data transmission security requirements</li> </ul>

#### (4) Document Approval History:

Date	Approver	Version	Reference
6/28/2021	Adam Solley – Senior Commercial Director	Version 1.1	Approved on behalf of the Information Security Committee
5/31/2022	Phillip Wood – Deputy CEO	Version 1.2	Approved on behalf of the Information Security Committee
8/10/2023	Sharon Turriff – Head of Legal, Commercial and IS	Version 1.3	Approved on behalf of Information Security Committee
2/6/2023	Mike Johns – CFO and Head of Information Security Committee	Version 1.4	Approved on behalf of DPO/ISC

DocuSigned by:

Mike Johns

8F13CF43181548A...

#### (5) Questions and Comments:

If you have further questions or would like additional information regarding Aptitude Software's Acceptable Use Policy, please contact:

---

## **Aptitude Software Group Plc – Acceptable Use Policy for Cloud Service Clients**

- Information Security Officer (ISO) at [information-security@aptitudesoftware.com](mailto:information-security@aptitudesoftware.com)
  - Aptitude Support [support@aptitudesoftware.com](mailto:support@aptitudesoftware.com)
-

## **Aptitude Software Group Plc – Acceptable Use Policy for Cloud Service Clients**

### **Table of Contents**

- **Scope**
- **Aptitude Cloud Services Definition**
- **Purpose of Cloud Services and Type of Data Hosting**
- **General Client Use Requirements**
- **General Aptitude Use Policy**
- **System and Organization Controls (SOC) Reporting and System Use**
- **Complimentary User Control Requirements for Clients**
- **Third Party (resellers, client contracted entities) Use Requirements**
- **Limitations on Client Use**
- **Remote Collaboration and Conferencing Tools**
- **Malware Detection Events**
- **System Availability Events**
- **Acceptable Use Policy Enforcement**

## Aptitude Software Group Plc – Acceptable Use Policy for Cloud Service Clients

### Acceptable Use Policy for Cloud Services

---

#### Scope

The Aptitude Software Acceptable Use Policy is applicable to cloud services provided by all Aptitude Software Group Plc subsidiaries including:

- Aptitude Software Group Companies
- MPP Global Group Companies

The collective organization is referred to as “Aptitude Software” and the associated cloud services are referred to as “Aptitude Software Cloud Services” throughout this document.

#### 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 transaction processing application software such as Aptitude Lease Accounting Engine(ALAE) or Aptitude RevStream (AREV), Cloud Aptitude Accounting Hub (AAH) solutions, Fynapse or eSuite.
- Application infrastructure elements including Amazon Web Services (AWS), Azure Cloud Services, database/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

#### Purpose of Aptitude Software Cloud Services and Type of Data Hosting

Table below lists the purpose and typical data hosted by Aptitude Software Cloud Services.

Service Category	Entity	Cloud Service	Purpose	Data Hosting Requirements
Category I	Aptitude Software Group	<ul style="list-style-type: none"> <li>• eSuite</li> </ul>	Subscription Management Software	<p><b>Data Included</b></p> <ul style="list-style-type: none"> <li>• Client Confidential Data</li> <li>• Client Subscriber data including personal data (non-sensitive data)</li> <li>• Client and Client Subscriber payment card data</li> </ul> <p><b>Data Excluded</b></p> <ul style="list-style-type: none"> <li>• Client Export Control Data</li> <li>• Client Sensitive Personal Data</li> </ul>
Category II	Aptitude Software Group	<ul style="list-style-type: none"> <li>• AREV</li> <li>• ALAE</li> <li>• AAH SaaS</li> <li>• Fynapse</li> </ul>	Revenue Management, Accounting and Financial Transaction Management Software	<p><b>Data Included</b></p> <ul style="list-style-type: none"> <li>• Client Confidential Data including financial data</li> </ul> <p><b>Data Excluded</b></p> <ul style="list-style-type: none"> <li>• Client Export Control Data</li> <li>• Client or client controlled Personal Data and Payment Card Data</li> </ul>

## Aptitude Software Group Plc – Acceptable Use Policy for Cloud Service Clients

As described in the table above, Category II Aptitude Software Cloud Services systems are NOT designed to process or store client personal data, personal health data, export-controlled data<sup>1</sup> or payment card data

### Client Data 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.
- Category II Aptitude Software Cloud Services systems are not designed to process or store client personal data (including health data), payment card data and export-controlled data<sup>1</sup>. 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.
- Aptitude Software generally does not permit users to perform security testing over Aptitude software. In the event such testing is required with a specific and limited focus, users are required to notify and seek the prior written approval of Aptitude Software Information Security or Aptitude Software Client Support ([information-security@aptitudessoftware.com](mailto:information-security@aptitudessoftware.com)) in advance of any potential or planned use of the cloudservices system by third parties including auditors, penetration testers or other service providers and vendors who are not contracted directly with Aptitude Software. Additionally, client users are required to authorize any service provider personnel who wish to access the system by contacting Aptitude Software Client Support at [support@aptitudessoftware.com](mailto:support@aptitudessoftware.com)

### Aptitude Data Use Policy

Aptitude Software classifies any data uploaded by the client into the cloud system or data generated due to client use of the cloud systems as client data. Per Aptitude Software policies, such client data may only be utilized for providing contracted cloud services to the client or for improving such services.

Aptitude Software will not disclose client data in response to demands from third parties including government entities unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is a clear indication of illegal conduct in connection with the use of Aptitude Software products or services, Aptitude Software will notify clients before disclosing client data.

### System and 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 production 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. SOC2 Type II reports may be provided for certain cloud services where relevant in addition to SOC1 reports.
- Prior to production service operation, a SOC 1 Type I for new services may be provided to enable clients to understand and align service controls to internal control requirements. Type II report for new services are expected to be available after within 12 months of production service operation.
- Further details regarding Aptitude Software's SOC program may be obtained at the following location <https://www.aptitudessoftware.com/security-trust-center/>
- Clients and user entities are required to comply with complementary control requirements identified within the service specific SOC1 reports.

---

<sup>1</sup> 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))

## 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 complimentary 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.
- where specified under SOC1 Complimentary User Control requirements, notify Aptitude Software with a request to perform client validation testing or User Acceptance Testing.
- where specified under SOC1 Complimentary User Control requirements, notify Aptitude Software when client validation testing is complete, thus approving that the testing was completed successfully and 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.
- Approving, administering, provisioning and de-provisioning, and performing a periodic review of individual user access (including user roles and third-party users) 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](mailto:information-security@aptitudesoftware.com).
- secure and monitor transmissions originating from user systems to Aptitude Software and ensure that any data in-transit from user systems to Aptitude Software is appropriately protected.
- 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 at 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.

## Third Party Use Requirements

Third parties include but are not limited to resellers and client contracted entities. Client contracted entities include but are not limited to implementation consultants and other service providers including managed service providers.

Client contracted third parties are treated the same way as clients by Aptitude Software and any use requirements which apply to clients are also applicable to client contracted third parties who have been provided access to cloud systems based on request and approval by clients. Clients are responsible for ensuring that any third parties contracted by them understand and agree with Acceptable Use Policy requirements.

Additional use requirements for third parties

- 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.
- Clients will ensure that 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 reseller or client contracted third party 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 with 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 Client 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 or other Security 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](mailto: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](mailto: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.