IT Security & Privacy FAQs

Class Super Pty Ltd

CONFIDENTIALITY

The information provided in this document and provided visually and verbally in relation to this document is the intellectual property and the confidential information of Class Super Pty Ltd, except where the information is in the public domain or as otherwise provided in this document.

By opening this document, the reader agrees to hold all information in strict confidence, not to make the confidential information available in any form to any other party, and to refrain from using the confidential information for any purpose other than as stated in this document or with the specific prior agreement of Class Super Pty Ltd, or as required to be disclosed by law or governmental direction or requirement.

Table of Contents

Class provides a managed service via hosted hardware and software. In the industry, this is known as the Software as a Service (SaaS) delivery model.

Our clients trust us with their valuable and confidential data, and it's natural for questions to be asked about its security, as well as the measures taken to ensure system availability.

Class strives to be open about our IT security policies and facilities. This document has been created to outline the IT Security Framework and overarching Privacy Policy that has been adopted to address these concerns.

1 Data Management

There are various aspects of data management that are natural concerns for a solution delivered as Software as a Service. The following items outline how Class addresses these concerns.

1.1 Where is the data stored?

All **Your Data***, which is your customer's data*, is stored in Australia.

Our production systems which store Your Data are spread across two hosting providers, Macquarie Telecom (MacTel) and Amazon (AWS), both residing in Australia.

At MacTel we use their internet connectivity, rack space and power. The system is run on equipment owned by Class. The data is stored in storage devices within the equipment owned and operated by Class. At AWS, we use their infrastructure completely.

In addition to this, data is replicated between MacTel and AWS, and between AWS availability zones for Disaster Recovery (DR). See section 2.3 and 2.4 for additional detail.

MacTel and AWS certifications and standards provide the highest level of surety that Class' data storage is only accessible to authorised staff.

Our Data, *which is information about you*, our subscribers, adheres to Class' Privacy Policy (see Section 7).

1.2 Who controls the data?

The data is controlled entirely by Class. If for any reason Class requires other parties to handle data (e.g. contractors and specialists) then appropriate reciprocal arrangements, such as Non-Disclosure Agreements, and adherence to Australian Privacy Principles are put in place to safeguard the data. Access to the data is only granted on an as required basis; the hosting organisation does not have access to the data. Even physical access is limited as Class' racks are located in locked cages.

1.3 Who owns the data?

The administrator (Class Licensee) owns the data even though it is held on Class' servers.

1.4 What if I want to take my data and leave?

Class provides full access to all of your fund and accounting data. Class allows users to export all their fund and report data in an XML format readable by Excel, web browsers and many other tools. Documents can be downloaded from the Document Management System (DMS).

1.5 What measures does Class take to prevent data loss?

Class has a replica of the production database stored on hardware located at MacTel. An automatic data replication service duplicates the production data in no greater than fifteen-minute intervals. Any production database residing in AWS is also replicated to another AWS availability zone.

1.6 Can I receive a manual/tape data backup at regular intervals?

Class runs a sophisticated tiered backup system that is architected to meet our strict Service Level Agreements, Recovery Points Objectives and Disaster Recovery requirements. Our database schema is proprietary and not suitable for external use so manual backups would not provide a "usable" client backup. See section ”Extracting all your data from Class” in the Online Help for Class’ standard process. Clients can additionally use our extensive APIs to obtain the data in a manner that is most useful to themselves.

2 System Availability

2.1 Network connectivity

Our hosting partners, MacTel and AWS, are highly regarded hosting providers that provide a managed network service with redundant Internet links. Class works on a more than 99% availability model excluding scheduled maintenance. Scheduled maintenance is notified in advance and carried out during non-peak periods.

No production services or data are located in Class’ offices, and therefore production services are unaffected if Class’ own internet connection were to fail.

2.2 Monitoring

MacTel & AWS monitor the availability of their services, namely power and network access. Class monitors all other aspects of system availability directly via an active monitoring system with alerts used to trigger a response when a parameter being monitored does not reside within general operational limits.

The monitoring system monitors a number of key parameters from basic equipment health and capacity metrics (CPU, I/O, disk space, network) up through the application stack to the operation of system sub-components and ultimately the availability of the external system to the user base.

Security and audit monitoring is also implemented and facilitates the security measures described below.

2.3 What happens if there is a hardware failure?

The most basic level of protection against hardware failure is implemented by the use of RAID redundancy for the key storage drives. In particular, the use of RAID 6 provides dual-parity that can recover from multiple drive failures.

The second level of protection is the availability of warm standby replicas of the database and other application servers. These are separate physical servers which are also located at MacTel or compute capacity available at different AWS availability zones. If a more substantial hardware failure occurs, then the operation of the entire system can be moved to these standby servers.

2.4 What happens if the entire datacentre fails?

Class maintains an entire off-site replica of the Class System on Amazon's Cloud infrastructure which is kept up-to-date using data updates shipped at a maximum interval of 15 minutes. This system addresses Class' Recovery Point Objective and leverages Amazon's extensive hardware redundancy via availability zones.

2.5 Total cost of ownership (TCO)

Class' technology value proposition is based heavily on its Infrastructure as a Service (IaaS) underpinnings. Attempting to replicate the level of security, scalability and access that Class' infrastructure provides would require a client to implement and maintain the following components and services:

- Redundant servers, firewalls, switches, communications links and power
- High frequency backups stored in multiple locations
- Security procedures covering regular penetration testing, operating system patching, application updates and incident response procedures
- Disaster recovery planning and business continuity procedures
- Monitoring of the entire system by an experienced IT team

3 System security

3.1 Privacy and access control

Class' entire system is based on the concept of access on a need-to-know basis only. This is coupled with the use of privileges based on individual credentials. These are mapped in a highly granular fashion to ensure an individual user has access to only the data that they are entitled to view and modify. Clients are entirely partitioned off from each other.

This is a logical partitioning. Our access control mechanism conforms to a rigidly implemented Business, Brand and Fund hierarchy. These elements permeate the system and prevent any unauthorised access.

Physical access to the data storage devices is similarly restricted to an as-required basis.

The "access on a need-to-know basis" principle is also applied to Class staff.

3.2 Intrusion protection procedures

The term Intrusion in this context applies to Systems and the Communications Channels that connect users to those systems.

As well as the access control mechanisms described above, a number of other measures are implemented to prevent intrusion:

- Firewalls – limit access to required protocols only
- Proactive patch and update installation for key security related components
- Use of Anti-Virus software
- Use of Intrusion Detection System (IDS) for the Feeds system

All connections containing private session data are protected using an RSA 2048 bits encrypted channel. The protocols used also confirm the servers' identities through the use of site certificates.

3.3 Layered architecture

The use of a layered architecture (with a clear separation of User Interface, Business Logic and Data Access code) prevents against most opportunistic intrusion techniques such as SQL injection. Appropriate validation is also used to guard against such attacks.

3.4 Penetration testing

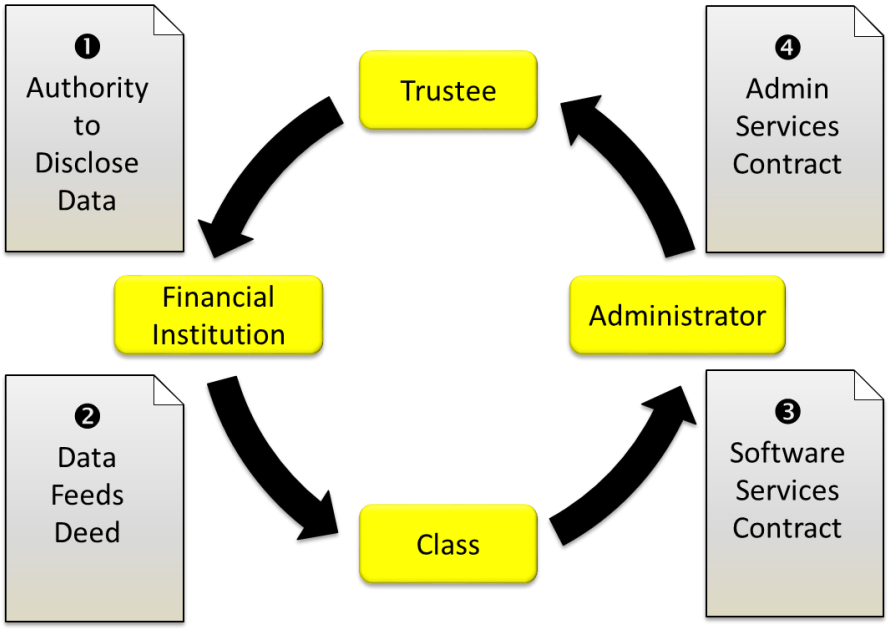
Whilst Class has implemented many architectural and operational measures to prevent security breaches, it is best practice to conduct Penetration Tests to verify the efficacy of those measures empirically. As such, Class ensures Penetration Tests are conducted on a regular basis.

4 Authority Legal Framework

The following legal framework has been adopted to protect all entities participating in the Class business processes.

4.1 What contracts protect my information legally?

The legal framework protecting an account holder's data is managed by the following agreements which cover rights, responsibilities, practices and procedures.



Agreements that make up the Data Feeds Legal Framework

4.2 What is the Authority Form?

The Authority Form is the legal agreement between the account holders trusted representative and the institution providing the account data. Unfortunately, there is no standard form or process for data feeds

activation as the Authority Forms are controlled by the institutions and not designed specifically for SMSF administrators' needs.

Financial institutions require their account holders to use a company specific data authority mechanism to send data to Class. The mechanism for authorisation varies from provider to provider but is typically a PDF form. Other mechanisms include online web activation, emails and phone based requests.

Forms do not usually include a way to acknowledge directly the role of the administrator and hence most forms only mention the receiver of the data e.g. Class.

a) Class does not send out authority forms direct to an account holder. Authority requests are intended to be sent directly from a trusted source e.g. the actual SMSF administrator.
b) Recommended practice is for the administrator to provide a cover letter with the authority forms explaining why the authority is sought, who Class is and explaining that the administrator will be the only Class user that will have access to that data.
c) The cover letter may also explain how to cancel the data feed (by sending a letter to the institution) and how it is compliant with Australian Privacy Principles. It may state or link to a privacy policy regarding the use, storage and protection of that data e.g. whether it is being sent offshore (though this may be covered in other service agreements).
d) The administrator is required to retain a copy of the authority form and needs to provide it on request to Class. The recommended practice is for the account holder to be directed to sign and return all authority forms to the administrator so that they can be checked, scanned, indexed and stored before on-forwarding to the relevant institution.
e) The administrator may also, at their discretion, explain the steps they have taken (as per point 1) to establish a contractual trust relationship with Class e.g. explain the due diligence process and service level agreements that they have put in place to protect the account holder.
f) Authority forms are not currently transferable and a new form is required to nominate a new administrator for access. Two administrators may have access concurrently.

Authority forms are not directly accessible and they must be generated so that Class can track when authority forms were sent. Unless the required fields are already on a form, Class may "overprint" the authority form with tracking fields (e.g. barcode and/or text) to identify the administrator and other details.

4.3 What is the Feeds Deed?

The Feeds Deed is signed by Class and the institution that is providing the data and acts as an umbrella agreement over the standard authority forms. Class uses a Feeds Deed to agree on the obligations and duties of each party in providing feeds. The Deed sets out the terms under which Class is being supplied data and conditions for its use including security, privacy and service level requirements.

4.4 What is the Class licence / Software Services agreement?

Administrators perform their own assessments, due diligence and sign a licence agreement with Class based on their assessment that Class can provide a secure, private and reliable service.

Administrators sign an agreement that includes terms and conditions for the use of the Class software. The terms of the contract require that:

> The Software must only be accessed and used by Authorised Users for the Approved Purpose and you must inform us immediately in writing of any changes in the Access Controllers.
>
> You are entirely responsible for the accuracy, quality, integrity, legality, reliability, appropriateness, and rights (including Intellectual Property Rights) of use in respect

of all of Your Data, including entering Your Data into the Software and maintaining Your Data. You must ensure that you have all necessary rights and consents for us to Process Your Data in accordance with this Agreement. You must ensure that Your Data and our Processing of Your Data in accordance with this Agreement does not give rise to any civil or criminal liability for us.

4.5 What is the Administration Services Contract?

SMSF administrators engage with Trustees under an Administration Services Contract further adding to and describing the legal framework in place.

An administrator can provide the Investor with access to Class screens that allow the client to have visibility of the data the administrator has access to. Class recommends that this access be granted but the use of this interface is at the administrator's discretion. Class plans to allow users to use this interface to nominate a new administrator and transfer data feeds authority; this functionality is not currently available and the account holder is required to complete new authority forms as noted above.

5 Authority Data Feeds

5.1 Who provides data to Class

Class currently receives data from over 185 different Brokers, Banks and Platform providers. If you want to receive data from a provider who is not on our current list of providers please let us know.

5.2 Where is my Feeds Data stored

Class places feeds data, on receipt, into a secure staging area or feeds warehouse. The data in the staging area is not accessible / visible to any administrator until the data has been matched and linked to a specific fund, at which time the administrator will be able to see the information as part of the specific fund data.

5.3 How does Class ensure the security and privacy of my account details?

The authority process, depending on the feed, requires all the correct credentials, including name, and wet signatures i.e. a completed Authority Form, before a provider will activate the feed that supplies Class with your account data. Within Class we provide further security filtering which can start with Adviser codes (if adviser / intermediary level authority) and then requires account details.

For account level authorities we also require authority forms match the barcodes we produce, which then need to be uploaded to Class before the feed activates. All of this ensures the correct feed is matched.

Additional rules, dependant on the account type and authority mechanism, are used to match and link accounts e.g. the account number must be correct, the product type must match, adviser credentials may be required etc.

6 Service Level Agreements

6.1 Who can call the Class Help Desk?

Any Class Licensee or person working for a Class Licensee can contact the Class Help Desk between 8:30am to 5:30pm, Monday to Thursday and 8:30am to 5:00pm Friday AEST to request assistance. Class will raise a support request for all contacts received and respond within the Call Window, or requiring service, according to the level of severity, see section 6.3 for more details on these classifications.

6.2 How can I log a support request?

Support requests can be logged through the Class application (when you've logged in, click on the life preserver icon, top right) or by emailing support@class.com.au. Class will respond to support requests, according to the level of severity.

6.3 What classifications are applied to support requests?

Classifications of calls are determined by the Class Support Officer as per the definitions below.

Severity	Description
Critical (Severity1)	Defined as the total inability to perform the normal operation of any significant business function where the result is that the majority of business group or groups cannot function properly and no workaround is available.
High (Severity 2)	Defined as a problem that severely restricts the use of Class software and is affecting a majority of system users and no workaround is available
Medium (Severity 3)	Defined as a problem which allows Class software to be used, but not at full capacity and results in a restriction that is not critical to the overall operation of the business or the department.
Low (Severity 4)	Defined as a problem, which relates to minor Class software problems where alternatives can be used. A Severity 4 problem does not require an immediate fix.

6.4 What are the agreed service levels?

Class will supply the Support Services in accordance with the target times in the table below but the Licensee is responsible for providing sufficient information and data to allow Class to readily reproduce all reported problems:

Severity	Response Timeframe	Update Every	Target Resolution	Escalation after
Critical (1)	1 business hour	2 hours or as agreed	4 business hours	30 minutes
High (2)	4 business hours	4 hours or as agreed	8 business hours	2 business hours
Medium (3)	12 business hours	As agreed	As agreed.	8 business hours
Low (4)	Before the end of the next business day	As agreed	As agreed.	As agreed

Further information on Class Support Services is available at https://www.class.com.au/education-support/class-support-services/

7 Class Privacy Policy

Class has the following Privacy policy (http://www.classsuper.com.au/privacy) which all clients agree to when they sign a licence agreement with Class.

8 Any Further Questions?

Please contact our support team on 1300 851 057.