Our Approach to Cyber Security & Data Protection Plan

Prepared for All Professional & Retail Clients of TPDCS

Date 01 July 2024 V 1.1

Prepared by *TPD Claim Support Pty Ltd

*TPDCS

TPD Claim Support Pty Ltd is a Corporate Authorised Representative No.001303179 of Axiis Capital Pty Ltd (AFSL 523464)

TPDCS Outsourcing and Data Security

TPDCS takes data security extremely seriously. TPDCS Information Security Management System is in line with all required industry standards with how we collect, store, & manage the data. The measures we take internally or the 3rd party professionals we outsource to, to ensure we maintain a diligent and robust system.

The data that TPDCS hold is classified as either Public, Protected or Confidential and as such, we ensure that necessary measures are in place to ensure the integrity of the data. This document outlines some of the data security measures that are taken, however we would be happy to discuss this with you further and provide documentary evidence upon request. We also hod data that is identified under legislation as Private or sensitive information as well as specifically managing numerous clients under the Life Codes Vulnerable Member definition which of course then holds significant risk if this data and information is collected, accessed, stored & managed without strong policy discipline and robust systems

TPDCS takes a holistic view to data security, including:

- Governance and Business controls
- Website
- Cyber security
- Access management
- Security monitoring and response
- ASIC privacy & Security Standards within an AFSL regime
- Training
- CRM – Hubspot

Governance and Business Controls

TPDCS have detailed Business controls in place. A comprehensive security policy is in place which is reviewed formally on an annual basis or sooner if an immediate matter arises that needs review. TPDCS also has a formal risk management framework to manage information security risks. All requirements required by ASIC within an AFSL are mandated as part of the TPDCS policy. Privacy, whether personal information or sensitive information have been considered and included in how we manage, store and access client data.

We also have access to leading technology which acts as part of our BCP policy, that enables us to ensure our data security is managed by professionals in this field. Our client data is stored on an external CRM, Hubspot, whose investment in cyber security and data security exceeds market expectations

The Hubspot Trust Centre publishes the extreme security measures they have on this link to ensure data integrity

HubSpot Trust Center | Powered by SafeBase

Essentially TPDCs mitigates risk by only allowing Employees to access Data via a TPDCS laptop, no mobiles phones or personal hardware or software. All data is stored on our CRM which requires an IT/Approved Admin approval and can be cancelled as part of a BCP or Risk matter immediately

Website

Our Website is managed by a 3rd party with no

- Access to data
- No data being stored on website
- No data being displayed on website.
- The website does not process, transmit or display any client data
- Any information such as a general query is delivered to the CRM or TPDCS email address

Cyber Security

All IT systems are encrypted to ensure that all data is communicated, transferred and maintained securely. All employee computers have 2 party authenticated security and no external hardware or software can be used by TPDCS employee or 3rd party's unless approved and in line with the security policy. Employees cannot put TPDCS data onto personal or 3rd party providers without a systematic internal approval process. TPDCS can only store data on approved external software that has an acceptable Cyber Security Management system that complies. Specifically for TPDCS our CRM, Hubspot.

Access Management

Privileged User Access is in place for all systems utilised by TPDCS . This is managed via detailed Information System Guidelines and no employee can access, manage or modify.

TPDCS has complex password requirements, which include 2 step authentication which are actively enforced to uphold the confidentiality and integrity of individual accounts. 2 step authentication has been enforced on all systems where available and the ability to access our CRM is via our TPDCS IT Admin authority and approval process. No 3rd party can access our CRM unless our Admin/IT Department approve and set up.

Security monitoring and response

TPDCS utilise Microsoft for active monitoring and management for Cyber security purposes as well as a 3rd party IT vendor to ensure we have controls and systems installed in all TPDCS hardware and software..

All employee computers and network equipment is centrally managed and monitored, or very specific controls in place to allow access to a 3rd party system such as our CRM

Physical premises are secured with building security guards, a BCP plan, security entry system, locked building entry and secured office entry as well as 24/7 CCTV footage and a "no mobile device" policy at desks.

Only approved, registered users of TPDCs can access our CRM.

TPDCS does not hold paper files of clients.

Training

TPDCS provides formal up front and ongoing training to all employees specifically in relation to information security. Additional training is provided to our business clients who may not understand this framework to ensure their roles are also responsible for Information Security.

CRM – Hubspot

TPDCS is committed to maintaining the integrity of its data. To ensure TPDCS remains up to date in an ever-changing landscape we also outsource and mitigate risk by adopting the use of a blue chip CRM that allows us to access Intellectual property and technology that invests and specialises in this area.

HubSpot specifically has a product feature that allows you to store sensitive data in certain places within your portal. This functionality allows TPDCS to store personal sensitive data, financial data, and/or Protected Health Information (PHI).

TPDCS & HubSpot is dedicated to the security, compliance and reliability of the products, the systems

They run on, and the environment which hosts those systems. HubSpot's security, privacy and compliance programs are published on this link;

HubSpot Trust Center | Powered by SafeBase