ASSOCIATED PROCESS SERVERS PTY LTD (the "Company")

Client Complaints Procedure

Our Complaints Policy

We are committed to providing a high-quality service to all of our clients. We aim to ensure that:

- Making a complaint is as easy as possible
- We treat your complaint seriously
- We deal with your complaint promptly and in confidence
- We learn from complaints and use them to review and improve our service

How to Make a Complaint

If you wish to make a complaint then you can contact your allocated Account Manager or alternatively our General Manager in any of the methods as below:

By email: at info@associatedps.co.uk

In writing: to Customer Services at

Customer Services
Associated Process Servers Pty Ltd
Level 25
Aurora Place
88 Phillip Street
Sydney NSW 2000

By phone: to Customer Services on 02 8310 4300

By fax: to Customer Services on 02 8310 4300

In person: to any of our offices

What will happen next?

1. We will send you a letter acknowledging receipt of your complaint within 3 working days of receiving it, enclosing a copy of this procedure.

2. We will then investigate your complaint and a response will normally be supplied within 10 working days of sending you the acknowledgement letter.

3. If you feel that your complaint has not been dealt with to your satisfaction then you can contact the Managing Director at:

   Managing Director
   Associated Process Servers Pty Ltd
   Level 25
   Aurora Place

88 Phillip Street
Sydney NSW 2000

4. If thereafter you still fee that your complaint has not been dealt with to your satisfaction then you can contact any appropriate governing body.

Comments

We are happy to receive any other comments on our service to clients.

Please contact us in any of the ways mentioned above or complete a comment card at any of our offices. Alternatively you can email us from the contact us section of our website.

ASSOCIATED PROCESS SERVERS PTY LTD (the "Company")

Information Security Policy

1. Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of the Company.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by the Company. This shall be achieved by:

- Ensuring that all members of the company staff are aware of and shall comply with relevant legislation, including the Privacy Act 1998.
- Describing the principles of information security management and describing how they shall be implemented within the company.
- Assisting staff to identify and implement information security as an integral part of their day to day role within the Company.
- Safeguarding information relating to staff and clients under the control of the Company.

2. Objectives

Key objectives of the Company Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those staff of the Company and relevant others with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the authorised individual or entity, when it is needed.

3. Responsibilities for Information Security

- Responsibility for information security shall rest with the Company. However, on a day-to-day basis the Managing Director shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The Managing Director shall be responsible for ensuring that both permanent and temporary staff including any contractors are aware of:-
  - The information security policies applicable to their work areas
  - Their personal responsibilities for information security
  - Who to ask or approach for further advice on information security matters.
- All staff shall abide by security procedures of the company. This shall include the maintenance of Company records whilst ensuring that their confidentiality and integrity are not breached (this applies to staff and company information. Failure to do so may result in disciplinary action.

- This Information Security Policy document shall be owned, maintained, reviewed and updated by the Managing Director. This review shall take place annually. The results of which shall be made known to the Managing Director.
- Staff of the Company shall be responsible for both the security of their immediate working environments and for security of information systems they use (eg workstations, laptops, PDAs, etc).
- Any contracts with third party organisations that allow access to the information systems of the Company, shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by the Company.

4. The Company shall undertake to ensure:

Contracts of Employment – address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

Access Controls - to areas containing information systems are restricted and controlled to ensure that only those authorised can access information of the Company.

Equipment Security – is effective in order to minimise losses, or damage to the Company. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked physical locations, clear desk policy and the limitation of risks in the surrounding work area etc).

Information Risk Assessment – a regular assessment of the working environment, shall be conducted to identify potential risks to the security of Company information. Where risks are identified, these should be noted and where possible mitigating action taken.

Security Incidents and weaknesses - are to be recorded and reported to the Managing Director so that they can be investigated to establish their cause, impact and the effect on the Company and its clients. (NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).

Protection from Malicious Software – should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the Company without the explicit permission of the Managing Director. Breach of this requirement may be subject to disciplinary action.

Secure Communications – should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of client records are conducted in a secure and confidential manner. The communication of confidential information by email must be appropriately protected, using appropriate automatic technical security protection.

Holding/Safeguarding/Disposal of Personal Data – data should not be held for longer than is necessary. Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary. Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure.

Business Continuity and Disaster Recovery Plans – are in place so that in the event of a disruption to the information services of the Company, it is possible to activate relevant business contingency plans until affected services are restored.

5. Staff Duties

Employees are expected to:

- Acquaint themselves with and abide by the Privacy Act 1988
- Read and understand this policy document.
- Understand how to conform to the standard expected at any stage in the life-cycle.
- Understand how to conform to the standard expected in relation to safeguarding data subjects' rights under the Act
- Contact the Data Protection Officer if in any doubt and not to jeopardise individuals' rights or risk a contravention of the Act.

6. Data Protection Principles

The company needs to keep certain information about its employees, customers and suppliers for financial and commercial reasons and to enable us to monitor performance, to ensure legal compliance and for health and safety purposes. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

7. Data Protection Contacts

Data Protection Officer/Managing Director
Associated Process Servers Pty Ltd
Level 25
Aurora Place
88 Phillip Street
Sydney NSW 2000
Tel. 02 8310 4300
E. info@associatedps.com.au

ASSOCIATED PROCESS SERVERS PTY LTD (the "Company")

Employee Vetting and Training Policy

Intention

The primary objectives of the policy are to safeguard our intelligence, operational and financial assets, and to preserve the health, safety and welfare of our staff and clients.

The policy forms part of a broader security strategy to complement measures to protect organisational assets and reduce the risk of loss or compromise. It is reinforced by a set of security standards and templates that explain requirements and provide guidance to support implementation.

General Principles

Vetting processes relate to 'role' and no distinction is made between different staff categories. However, different roles require different levels of vetting and the appropriate clearance process will be completed before new applicants (internal or external) are appointed to a role.

Vetting clearance is based upon circumstances at a particular time and, in any event, lasts for a defined period only. Therefore, to continue to provide assurance as to the integrity, reliability and trustworthiness of individuals who have access to Company assets, 'aftercare' procedures are necessary and these will include renewal, annual assessment for some roles, and review of a change of circumstances.

Role Assessment

The Managing Director will assess roles to specify the appropriate level of vetting. New roles or significant variations to existing roles will be notified to the Managing Director for review. A record of the role related vetting level will be recorded on the personnel computer system.

Identification and Residency

Part of the vetting process involves the applicant producing documents to prove their identity and place of residence. In addition, to allow meaningful vetting checks to be completed, a minimum period of two years residency in the Australia is required. Applicants for designated posts must demonstrate a minimum period of two years residency in the Australia.

Vetting Decisions

Every case is reviewed individually and if any doubt exists about the granting of vetting clearance, the circumstances are referred to the Managing Director before refusal is confirmed.

Checks, underpinned by all current legislation and regulations, may include:

- Identity checks must be carried out on all appointments to the Company's workforce before the appointment is made.
- Checks to confirm that qualification requirements are met.
- Checks to confirm that driving qualification requirements are met.
- Assessment by the Company's representative as to the employee's overall general suitability to perform the relevant role.

Training

All new employees are provided with a level of training commensurate with the role for which they are employed which may include one-on-one supervision for a period of time, daily review of performance, unlimited access to managerial level advice or other suitable training as deemed appropriate by the Company.

Regular and ongoing training as to any revisions in practice or legislation is provided to all employees to maintain an appropriate level of knowledge and performance.

Aftercare

Vetting clearance may be varied from time to time and a series of measures may be adopted to renew or confirm the validity of vetting. The measures include:

- Ongoing supervision
- Notification and review of change of personal circumstances
- Annual assessment
- Business interest review

Data Protection

All personal information supplied will be processed in accordance with the Privacy Act 1988. This prohibits any person, knowingly or recklessly, from disclosing personal data or information contained within personal data, without the consent of the Company or its appropriate representative.

Monitoring and Review

This policy will be reviewed annually and will take account of relevant legislation, national policies and procedures.

ASSOCIATED PROCESS SERVERS PTY LTD (the "Company")

General Ethical Policy

The Company conducts its business according to rigorous ethical, fair, professional and legal standards.

It flows from our determination to:

•Be fair
•Be transparent
•Be accountable
•Be honest
•Be cautious
•Be thorough
•Be law abiding
•Be mindful of the confidentiality of that with which we are entrusted

Principle 1- Responsibility and Accountability
The Company is responsible and accountable for its actions or omissions.

Principle 2 - Honesty and Integrity
The Company is to act with honesty, integrity and must not compromise its position or any of its clients.

Principle 3 - Caution and Thoroughness
The Company will endeavour where appropriate to verify the credentials of clients in order to ensure that they have lawful and moral reasons to request an investigation or provision of any service by the Company.

Principle 4 - Conflict of Interest
Any personal or conflicting interest in any matter in which the Company is involved shall be disclosed if it is in conflict with the interests of their clients.

Principle 5 - Acting within the Law
The Company is to obey the law and refrain from carrying out any act that it knows, or ought to know, is unlawful.

Principle 6 - Authority, Respect and Courtesy
The Company is not to abuse its position and must respect the rights of all individuals.
The Company is to act with self-control and tolerance, treating everyone with whom they come into contact, during the course of their activities, with respect, fairness and courtesy.

Principle 7 – Equality
The Company is to act with fairness and impartiality. It will not discriminate unlawfully on the grounds of sex, race, colour, language, religion or belief, political or other opinion, national or social origin, association with a national minority, disability, age, sexual orientation, property, birth or other status.

Principle 8 – Confidentiality
The Company is to treat information with which they are entrusted during the course of business with respect and access or disclose it only for the purposes for which it is intended; attending to all instructions within the principles of the prevailing privacy legislation and in particular if controlling personal data to be so notified with the Information Commissioner.

Principle 9 - General Conduct
The Company is to act in a professional manner.

ed Process Servers Pty Ltd

Organisational Chart