1. ABOUT THIS POLICY

1.1 Easec Pty Ltd understands the importance of ensuring the highest standards of privacy in all operations across the organisation. Easec collects, manages, uses and discloses personal and sensitive information strictly in accordance with the Australian Privacy Principles (the APPs) and the Privacy Act 1988 (the Privacy Act). A copy of the APPs is available at Appendix A.

1.2 This Policy outlines how Easec protects the information it holds from misuse and loss and from unauthorised access, modification or disclosure.

1.3 Easec may update this privacy policy without notice at its discretion, including when our information handling practices or applicable laws change. Updates will be made available through the Easec website.

1.4 By continuing to access our services, you consent to us collecting, holding, using and disclosing your personal information in accordance with this Policy.

2. COMMENCEMENT

2.1 This Policy will commence from 5 August 2020. It replaces all other Privacy Policies of Easec (whether written or not).

3. APPLICATION

3.1 This Policy applies to personal information collected by Easec in respect of its clients, prospective employees, current and prospective agents, consultants and contractors (including temporary contractors) of Easec but does not apply to personal information contained in employee records (as defined in the Privacy Act).

3.2 It is a condition of Easec employees' contracts of employment that this Policy is to be adhered to at all times.

3.3 Under the Privacy Act, personal information is any information or an opinion about an identified individual or an individual who can be reasonably identified from the information or opinion. Information or an opinion may be personal information regardless of whether it is true.

4. RESPONSIBILITIES

4.1 It is the responsibility of all Easec' employees to manage personal information in accordance with this Policy.

4.2 It is the responsibility of the Easec Team Leaders and Account Managers to identify and report any privacy concerns or risks to the Easec General Manager, in conjunction with the risk management policy and procedures.

4.3 It is the responsibility of the Easec Team Leaders and Account Managers to implement and monitor changes to Easec processes as a result of identified and validated privacy risks within Easec.

4.4 It is the responsibility of the Easec General Manager to make and approve changes to this Policy.

5. TYPES OF PERSONAL INFORMATION COLLECTED AND HELD

5.1 The type of personal information we may collect and hold differs depending on the nature of our interaction with you.

5.2 Sensitive information is a subset of personal information and includes personal information that may have serious ramifications for the individual concerned if used inappropriately. For example, sensitive information may include but is not limited to:

5.2.1 health or genetic information;

5.2.2 racial or ethnic origin;

5.2.3 sexual orientation or practices;

5.2.4 criminal record;

5.2.5 political opinions or associations;

5.2.6 religious or philosophical beliefs; and

5.2.7 trade union membership or associations.

5.3 We will not collect sensitive information without the individual's consent to whom the information relates unless permitted under the Privacy Act.

5.4 Personal information collected and held about clients may include and is not limited to:

5.4.1 name, address, date of birth, phone number, email address, next of kin;

5.4.2 history of purchases and use of our services;

5.4.3 details of enquiries or complaints made;

5.4.4 banking details;

5.4.5 credit card or payment details;

5.4.6 government related identifiers such as Medicare numbers;

5.4.7 sensitive information such as health information; and

5.4.8 any other personal information required to provide services to you.

5.5 Personal information collected and held about prospective employees and current and prospective contractors, consultants and agents may include and is not limited to:

5.5.1 name, address, date of birth, phone number, email address, next of kin;

5.5.2 employment information (current and previous);

5.5.3 education information;

5.5.4 photographs of the individual in their workplace or home environment (for Workplace Assessment of Activities of Daily Living Assessment);

5.5.5 Government related identifiers such as tax file numbers;

5.5.6 sensitive information such as health information, criminal history, membership of professional or trade associations, membership of trade unions, racial or ethnic origin and biometric information; and

5.5.7 any other information required for engagement of employees, contractors or agents.

6. METHODS OF COLLECTING PERSONAL INFORMATION

6.1 Generally, Easec will collect personal information directly from the individual to whom the information relates.

6.2 For example, Easec will collect Personal Information via face to face consultation, phone, email, in writing and online forms.

6.3 Easec may also collect personal information from third parties including, but not limited to:

6.3.1 treating doctors, specialists;

6.3.2 treating allied or other health professionals;

6.3.3 referring individuals, organisations or bodies;

6.3.4 employers (previous or current);

6.3.5 our employees, contractors, consultants and agents; and

6.3.6 government bodies.

7. ANONYMITY AND PSEUDONYMITY

7.1 The individual has the option of not identifying themselves or of using a pseudonym unless Easec are required or authorised under Australian law or a court/tribunal to identify the individual or it is impracticable to deal with the individual anonymously or by a pseudonym.

7.2 Easec allocates unique case numbers to all individuals for internal use only, in order to effectively manage case records including file notes, reports and case records.

7.3 If an individual decides not to provide their personal information, Easec may not be able to deliver its services or otherwise engage with that person.

8. INFORMATION STORAGE

8.1 Our usual approach to holding personal information includes physically, in paper files stored securely at our premises and electronically, in computer system and databases either operated by us or our external service providers.

8.2 We implement and maintain processes and security measures to protect personal information which we hold from misuse, interference or loss, and from unauthorised access, modification or disclosure.

8.3 Some of these processes and systems include:

- 8.3.1 using security cards or access codes to access areas that contain personal information;
- 8.3.2 using security cards to access printers;
- 8.3.3 using secure servers to store personal information;
- 8.3.4 using unique usernames, passwords and other protections on systems that can access personal information;
- 8.3.5 arranging for our employees to complete training about information security;
- 8.3.6 holding certain sensitive documents securely; and
- 8.3.7 monitoring and reviewing our policies.

8.4 Easec will generally maintain records of all information for a period of seven years. Documentation and personal records are managed in line with the Records Management Procedure.

9. OVERSEAS DISCLOSURE

9.1 Easec generally holds all personal information it collects within Australia.

9.2 All information storage platforms used by Easec are located in Australia. For example, personal information is stored on Microsoft SharePoint and OneDrive, as well as case management software Case Manager by Chameleon software.

9.3 All new information storage platforms are vetted through the Vendor Management Policy to ensure all information always remains onshore. Easec will not knowingly disclose personal or sensitive information to overseas recipients.

10. PURPOSES FOR COLLECTING, HOLDING, USE AND DISCLOSURE OF PERSONAL AND SENSITIVE INFORMATION

10.1 The primary purposes for which we collect, hold, use and disclose personal information varies depending on the individual that we are collecting the information from but is generally as follows:

- 10.1.1 in the case of clients, to provide our services including the provision of assessment, return to work and rehabilitation assistance;
- 10.1.2 in the case of a current contractors, consultants or agents, to assist us in providing our services; and
- 10.1.3 in the case of prospective contractors, consultants, agents or employees, to assess suitability for employment or engagement.

10.2 Easec may also collect, hold, use and disclose personal information for secondary purposes that are within a person's reasonable expectations and that are related to the primary purpose.

10.3 Should the information need to be used to an alternative purpose express consent will be obtained from the individual.

11. ACCESSING AND CORRECTION OF PERSONAL INFORMATION

11.1 All individuals have the right to request access to their personal information and to request its correction, including adjusting or withdrawing their consent.

11.2 Easec adheres to the Freedom of Information Act 1982 (FOI Act) which operates alongside this Privacy Policy and does not replace other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information, including the FOI Act.

11.3 Should any individual wish to access or request a correction of their personal information they should contact their direct consultant or the person specified below. All requests must be sent in writing for consideration.

General Manager
Ms Julia Bunn
165 Kelvin Grove Road, Kelvin Grove QLD 4059
(07) 3366 2123
info@easec.com.au

11.4 Easec will endeavour to respond within a reasonable period after the request is made (no more than 10 business days after the request is received) and provide access to or correct the personal information in the manner requested where reasonable and practicable to do so.

11.5 Easec may charge an administrative fee for the reasonable costs of providing a copy of the information requested.

11.6 In keeping with our commitment to protect the privacy of personal information, we may not disclose personal information to you without proof of identity.

11.7 We may deny a request to access personal information if:

11.7.1 the request is unreasonable;

11.7.2 providing access would have an unreasonable impact on the privacy of another individual;

11.7.3 providing access would pose a serious and imminent threat to the life or health of any person; and

11.7.4 there are other legal grounds to deny the request.

11.8 If access to personal information is refused, or access in the manner requested is refused, Easec will write to the individual to inform them of the reasons why (unless unreasonable to give reasons having regard to the grounds of refusal) and the complaints process.

11.9 Easec will not provide any individual or any other party, reports received from third parties without the written consent of the third party in question. Requests for such information will be referred to the relevant author of the report or the third party in question.

11.10 Easec may also provide information to other parties in the case where:

11.10.1 Easec believes it is necessary to assist an enforcement body to perform its functions.

11.10.2 Easec suspects that an unlawful activity has been, is being or may be engaged in and the personal information is a necessary part of our investigation or reporting of the matter.

11.10.3 Easec reasonably believes it is necessary to prevent a threat to life, health or safety

11.10.4 Easec is authorized or required by law to do so, (e.g. where information is required by bodies regulating Easec or in response to subpoenas or warrants)

11.10.5 Easec has contracted an external organisation to provide support services and that organisation has agreed to conform to our privacy standards.

12. PRIVACY COMPLAINTS

12.1 Individuals who wish to submit a complaint to Easec must do so in writing for consideration.

12.2 Easec will endeavour to respond within a reasonable period after the complaint is received (no more than 30 days after the complaint is received) and address the complaint where reasonable and practicable to do so.

12.3 The complaint should be sent to:

General Manager
Ms Julia Bunn
165 Kelvin Grove Road, Kelvin Grove QLD 4059
(07) 3366 2123
info@easec.com.au

12.4 Should the individual or any Easec employee feel the complaint has not been resolved, or the complaint has not been responded to within 30 days of submission, they can then complain to the Office of the Australian Information Commissioner. Further information on this can be found at: http://www.oaic.gov.au/privacy/making-a-privacy-complaint. Information about the Australian Privacy Principles can be found at: http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles.

13. DOCUMENT MANAGEMENT

13.1 This draft was approved by Julia Bunn, General Manager

14. VARIATIONS

14.1 Easec reserves the right to vary, replace or terminate this document, without notice, from time to time.

14.2 Changes to this policy will be made in conjunction with the following:

14.2.1 Changes to Australian state or federal legislation

14.2.2 Changes to industry standards of regulatory bodies

14.2.3 Changes to Easec corporate governance requirements

14.2.4 Changes to Easec stakeholder corporate governance requirements which impact Easec.

14.2.5 Any other change to procedure or requirement which Easec deem reasonable to implement, whilst adhering to the relevant legislation and requirements.

15. RELATED DOCUMENTS

15.1 Data Breach Policy and Procedure

15.2 Consent Form

15.3 Privacy Brochure

15.4 Complaints Management Policy and Procedure

15.5 Records Management Procedure

15.6 Communications Procedure

APPROVED BY

Julia Bunn, Manager Director

VARIATIONS

Easec reserves the right to vary, replace, or terminate this Code from time to time.

APPENDIX A

AUSTRALIAN PRIVACY PRINCIPLES

Further information on each principle is available on the Office of the Australian Information Commissioner website.

Principle	Title	Purpose
1	Open and transparent management of personal information	Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.
2	Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
3	Collection of solicited personal information	Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.
4	Dealing with unsolicited personal information	Outlines how APP entities must deal with unsolicited personal information.
5	Notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.
6	Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
7	Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
8	Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
9	Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.
10	Quality of personal information	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
11	Security of personal information	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
13	Correction of personal information	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.