Policy for the Protection of Privacy

Executive Summary

This document sets out the principles that Ace Internet Services Pty Limited (AIS) will adopt in order to protect information about individuals. These principles are consistent with the National Privacy Principles contained in Schedule 3 of the Privacy Act and are similar to those outlined in the Australian Communications Industry Forum Privacy Code. These principles deal with the collection, use, disclosure, storage and transfer of personal information as well as access to information. In addition, this procedure document also sets out the principles that AIS will adopt when considering the introduction of new technology or services.

For each principle, procedures have been set out to provide guidance for the application of that principle by AIS employees, agents and contractors. The principles are interrelated and should be read in conjunction with the procedures that follow each principle.

AIS's Privacy Protection Principles reflect customers' privacy concerns in four key areas relevant to telecommunications as follows:

a. Communications
   Users of telecommunication services expect their communications to be kept private and confidential.
b. Customer and employee information
   Customers, including the customers of other telecommunication carriers and service providers, and AIS employees, expect telecommunication companies to respect the privacy of the personal information obtained from them, generated from their use of services, or obtained from third parties.
c. New Products and Services
   The impact of new products and services on privacy of customers is a fundamental issue to be considered in the design, introduction and operation of all new products and services.
d. Privacy and the Regulatory Environment
   The Australian Communications Authority (ACA), the Federal Privacy Commissioner and the Telecommunication Industry Ombudsman (TIO) actively monitor privacy in the Australian telecommunications industry. A summary of their roles is set out below.

Telecommunications Act 1997

Privacy protection in the Australian Telecommunications industry is required by the Telecommunications Act. Part 13 of the Telecommunications Act requires amongst other things that carriers, carriage service providers and their employees (amongst others) must protect the confidentiality of information relating to:

a. other contents of communications that have been, or are being carried by carriers or carriage service providers;
b. carriage services supplied by carriers or carriage service providers; and
c. affairs or personal particulars of another person.

Protected information may be used or disclosed in limited circumstances specified in the Act. The Act also restricts the secondary use/disclosure of information and imposes record keeping requirements.

Privacy Act 1988

From 21 December 2001, the Privacy Act 1988 ("Privacy Act") will contain a separate privacy scheme for the private sector. This will be in addition to the provisions relating to the Commonwealth public sector, credit reporting and tax file numbers.

The Privacy Act requires AIS to comply with the National Privacy Principles in the collection, storage, use, correction, disclosure or transfer of personal and sensitive information.

Personal and sensitive information may only be collected if necessary for one or more of AIS's functions or activities and must be collected only by lawful and fair means. Personal and sensitive information may only be used or disclosed in limited circumstances specified in the Privacy Act. Secondary use/disclosure is also restricted by the Privacy Act and specific access/correction requirements are imposed.

ACIF Privacy Code

The ACMA is a statutory authority established under the Australian Communications and Media Authority Act 1997 to act as an independent regulator of Australian telecommunication carriers.

The Telecommunications Act also provides for the development and registration by the ACMA of industry codes and standards. The ACIF Privacy Code has been registered by the ACMApursuant to section 117 of the Telecommunications Act 1997. All telecommunications providers are required to comply with the ACIF Privacy Code.

AIS's Privacy Protection Policy is consistent with the National Privacy Principles and complies with the ACIF Privacy Code. That Code will continue to apply until deregulated.

The Telecommunications Industry Ombudsman

The TIO Scheme was established in 1993 to provide independent resolution of customer complaints, including complaints concerning interference with the privacy of an individual in terms of non-compliance with the Information Privacy Principles contained in s14 of the Privacy Act, which applies to certain Commonwealth Government bodies, or any industry specific privacy standards which may apply from time to time.

All Australia's carriers and carriage service providers are required to be participants in the TIO scheme, which operates independently of government, carriers and other interested bodies.

Customer complaints regarding telecommunication carriers should first be referred to the carrier in question. If the matter cannot be satisfactorily resolved, it may then be referred to the TIO's office for resolution.

Under s114 of the Telecommunications Act, industry codes and standards may confer powers on the TIO. Complaints from individuals who believe that their privacy has been interfered with will be addressed through AIS's internal complaint handling procedures.

If the matter cannot be satisfactorily resolved, within a reasonable period of time, the individual concerned can seek the assistance of the Telecommunications Industry Ombudsman.

Federal Privacy Commissioner

The Federal Privacy Commissioner administers the Privacy Act and oversees regulation of privacy in the private sector under the Privacy Act. One of the important functions of the Federal Privacy Commissioner is to encourage corporations, such as AIS, to develop programs for the protection of personal information which are consistent with internationally accepted data protection standards.

It is AIS's procedure to consult with the Privacy Commissioner on issues with significant privacy implications.

Under the Telecommunications Act the Privacy Commissioner is responsible for monitoring compliance with the record keeping requirements imposed under the Telecommunications Act.

Direction

The principles and procedures apply to all personal information under AIS's control including personal information held by each of AIS's agents, contractors and service providers.

Where AIS's agents, contractors or service providers are required to refer to this document, references to 'AIS' are to be taken to include references to those agents, contractors or service providers. AIS is subject to privacy obligations contained in Australian legislation and telecommunication regulations

AIS's Privacy Protection Principles & Relevant Procedures

Collection

1. AIS will only collect personal information that is necessary for one or more of its functions or activities.
2. AIS will only collect personal information by lawful and fair means and not in an unreasonably intrusive way.
3. At or before the time (or, if that is not practicable, as soon as practicable thereafter), AIS collects personal information about an individual from the individual, AIS will take reasonable steps to ensure that the individual is aware of:
    1. the identity of AIS and how to contact it;
    2. the fact that he or she is able to gain access to the information;
    3. the purposes for which the information is collected;
    4. the organisations (or the types of organisations) to which AIS usually discloses information of that kind;
    5. any law that requires the particular information to be collected; and
    6. the main consequences (if any) for the individual if all or part of the information is not provided.
4. If it is reasonable and practicable to do so, AIS will collect personal information about an individual only from that individual.

5. If AIS collects personal information about an individual from someone else, AIS will take reasonable steps to ensure that the individual is or has been made aware of the matters listed under clause 3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

Procedures: Collection not to intrude to an unreasonable extent.

When collecting personal information AIS will not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Specified purposes and limitation of collection

An individual will not be required to provide information beyond that reasonably required to fulfil the purposes for which the information is collected. Personal information will only be collected for specified purposes. The specification of a purpose will be sufficient to properly identify the purpose, as well as the information to be obtained, the nature of the consent required, how the information is to be collected, to whom the information may be disclosed and its retention, storage and disposal requirements.

Notifying the purpose of collection

Where personal information is to be collected directly from any individual, reasonable steps will be taken to ensure that the individual is aware of the purpose of collection. In many situations the purpose of collection will be readily apparent to the person concerned. In other circumstances it will be necessary to provide sufficient additional information to enable the person concerned to understand the purpose of collection.

If at the time of collection it is not feasible to notify the person concerned of the purpose of collection, then AIS will, as soon as practicable after collection, take reasonable steps to ensure the person is or has been made aware of the purpose.

Personal information obtained from third parties

When personal information is obtained from third parties, such information will be limited to that required for the identified purpose and will be collected by lawful and fair means for purposes directly related to AIS's activities.

Lawful and fair means

AIS will only collect personal information by lawful means and by means that do not mislead or deceive the person concerned or any third party. AIS will inform customers of any significant consequences of not providing information.

Notification of Usual Disclosure Practices

If appropriate and practicable to do so, individuals will be notified of any usual disclosure practice of AIS for the personal information being collected. The notification will be provided at the time of collection or as soon as practicable after the collection has occurred.

Use & Disclosure

AIS will only use or disclose personal information about an individual for a purpose other than the primary purpose of collection (a secondary purpose) if

1. both of the following apply:
    1. the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
    2. the individual would reasonably expect AIS to use or disclose the information for the secondary purpose;
2. the individual has consented to the use or disclosure:
3. or the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
    1. it is impracticable for AIS to seek the individual's consent before that particular use; and
    2. AIS will not charge the individual for giving effect to a request by the individual to AIS not to receive direct marketing communications;
    3. the individual has not made a request to AIS not to receive direct marketing communications;
    4. in each direct marketing communication with the individual, AIS draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications;
    5. each written direct marketing communication by AIS with the individual (up to and including the communication that involves the use) sets out AIS's business address and telephone number and, if the communication with the individual is made by fax or other electronic means, a number or address at which AIS can be directly contacted electronically;
4. the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
    1. it is impracticable for AIS to seek the individual's consent before the use or disclosure;
    2. the use or disclosure is conducted in accordance with guidelines approved by the Privacy Commissioner under section 95A of the Privacy Act for the purposes of this subparagraph;
    3. in the case of disclosure – AIS reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information;
5. AIS reasonably believes that the use or disclosure is necessary to a serious and imminent threat to an individual's life, health or safety; or a serious threat to public health or public safety;
6. AIS has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;
7. the use or disclosure is required or authorised by or under law; or
8. AIS reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
    1. the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
    2. the enforcement of laws relating to the confiscation of the proceeds of crime;

3. the protection of the public revenue;
4. the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
5. the preparation for, or conduct of, proceedings before any court or tribunal, implementation of the orders of a court or tribunal.

If AIS uses or discloses personal information under clause 8 above, AIS will enter the disclosure event into a register for statutory reporting purposes.

Procedures relating to use and disclosure

These procedures relate to the use and disclosure of personal information internally within AIS, irrespective of whether that information was collected directly from the individual concerned, generated through the individual's use of the network or other business relationship or obtained from third parties. These procedures are consistent with Part 13 of the Telecommunications Act, but should there be any doubt that the proposed use of information is permitted by Part 13, the matter should be discussed with AIS's Company Secretary. Wherever feasible, personal information will be made anonymous prior to its use for any purpose.

Use in the performance of duties

AIS employees, agents and contractors are only authorised to access or use personal information in the legitimate performance of their duties.

AIS employees, contractors and agents are not permitted to access customer information for any purpose other than performance of their duties. “Browsing” is not permitted under any circumstances. AIS employees, contractors and agents must comply with all reasonable directions given by AIS in relation to their use of, and access to, personal information.

Use for primary or directly related purposes

Personal information may be used for a purpose specified at the time of collection (primary purpose) or for other purposes related to that purpose (secondary purposes) provided that a customer would reasonably expect AIS to use the information for that secondary purpose. Personal information may also be used where the customer has given express or implied consent. Where personal information is collected for the provision of a telecommunications service the subsequent use of that information for network planning, installation, operation and maintenance purposes should be regarded as a use for related purposes. In all other cases the assessment of whether a proposed use is directly related to the purpose specified at the time of collection and within the reasonable expectations of the customer will be made on a case by case basis.

Improvement of customer service and direct marketing

Personal information may be used to the extent necessary to improve customer service, including product development, market research and marketing, where that use is related to the purpose of collecting the information and within them reasonable expectations of the customer. The assessment of whether a proposed use is related to the purpose specified at the time of collection and within the reasonable expectations of the customer will be made on a case by base basis. An example of a legitimate use for a

secondary purpose would be using the information on a customer's phone bill to inform the customer of a discount available on calls to a frequently called location.

The use of personal information to assist in direct marketing of services or products which are unrelated to the services or products originally supplied to the customer will be undertaken in accordance sensitivity (refer 3 above). That is where the proposed use of personal information is for direct marketing purposes and such use is not a legitimate secondary use as outlined above. AIS will only undertake such use with the express consent of the person concerned or, if that is impracticable, AIS will advise the customer of the use at first contact and offer the customer the opportunity to opt-out of further marketing uses.

In addition to the above, AIS will conduct its direct marketing and market research activities in accordance with accepted industry standards and its procedure for direct marketing.

AIS will maintain a record of individuals who have requested that AIS not contact them for direct marketing purposes. Personal information will not be used for contacting the individual for direct marketing purposes where the individual has indicated that they do not want to be contacted for those direct marketing purposes.

Intrusion

AIS recognises that a balance should exist between the legitimate use of unsolicited communications and their potential for intrusion into personal privacy.

Derivation of anonymous or aggregated information

Personal information may be used to the extent necessary for the creation and use of records (including databases), provided that the individual concerned can no longer be readily identified and the record cannot be de-aggregated or associated with an individual once it has been created.

Threat to life or health

Personal information may be used or disclosed where it is reasonably necessary to do so and in circumstances where it is believed that there is a serious and imminent threat to the life or health of the individual concerned or of another person or public health or safety. Where personal information is used or disclosed for this purpose, a record of the circumstances will be retained.

Use where permitted by law

Use of personal information is only permitted in accordance with company policies and procedures or otherwise as permitted under sections 279 to 293 of the Telecommunications Act or under the Privacy Act. In circumstances where use may be required or authorised by or under law, AIS will ensure that the use is lawful and that personal information is only used to the extent required.

Disclosure for law enforcement purposes

AIS will disclose personal information to officers and authorities of the Commonwealth, States and Territories when it is reasonably necessary for any of the following purposes:

1. enforcing the criminal law and laws imposing pecuniary penalties,
2. protecting the public revenue,
3. Safeguarding national security.

Such disclosures will be strictly in accordance with company policies and procedures or as otherwise directed by the Company Secretary. Where personal information is disclosed for law enforcement purposes or for the protection of public revenue, a record will be made into a register for statutory reporting purposes. AIS will usually request an agency to provide certification under s282 of the Telecommunications Act that the disclosure is reasonably necessary. However, if no certification is provided, AIS will make an assessment as to whether, in the circumstances, the disclosure should be made. Except as required by law, AIS will not disclose personal information to customers for their personal law enforcement purposes.

Consent

Depending on the circumstances, consent for the use or disclosure of personal information may be express or implied. Generally, express consent will be obtained where the information is likely to be considered sensitive, taking account of the proposed use and the reasonable expectations of the individual concerned. Consent may be withdrawn at any time, but not with retrospective effect. The individual concerned will be informed of the consequences of withdrawing their consent.

Employment data

AIS will only use employment information to the extent required by the proper discharge of its employment obligations and appropriate management of its human resources. Access to employment information will be restricted to those needing access for the proper performance of their duties.

Credit information

AIS will comply with the Credit Reporting obligations set out under Part III A of the Privacy Act and those set out in the Code of Conduct issued under the authority of the Privacy Act. AIS will also comply with any industry Credit Code developed under Division 3 of Part 6 of the Telecommunications Act.

Old Criminal Convictions

AIS will comply with the provisions of the Crimes Act 1914 which apply safeguards to the use of information about old minor, minor, and spent criminal convictions.

Consent for disclosure to third parties

Unless falling within one of the other exceptions set out in this principle, the disclosure of personal information to a third party will only occur with the consent of the person concerned. Depending on the circumstances, consent for the disclosure of personal information may be express or implied. Generally, express consent will be obtained where the information is likely to be considered sensitive, taking account of the nature of the proposed disclosure and the reasonable expectation of the individual concerned. Where oral consent is given, a notation to this effect will be appended to the information held by AIS. Consent may be withdrawn at any time but not with retrospective effect. The individual concerned will be informed of the consequences of withdrawing their consent.

Disclosure to an agent or contractor of AIS

Disclosure of personal information to an agent or contractor of AIS is permitted only to the extent necessary for the agent or contractor to be able to undertake or perform their contractual obligations.

Record Keeping of Disclosures

AIS will maintain a record of disclosures, where required to in accordance with Part 13 Division 5 of the Telecommunications Act, within 5 days of the disclosure being made and the record will be kept for a period of 3 years. The Privacy Commissioner is responsible for monitoring compliance with this record-keeping requirement.

Data Quality

AIS will take reasonable steps to make sure that the personal information it collects uses or discloses is accurate, complete and up-to-date.

a. AIS will use its best endeavours to ensure that personal information is accurate, complete and up-to-date when such information is collected, used or disclosed.
b. Where personal information is collected from the individual concerned it will generally be assumed to be accurate, complete and up to date, at the time of collection, unless there is other information which suggests that it is not.
c. Greater care will be exercised to determine the accuracy, completeness and currency of personal information collected from other sources.
d. Personal information will not be routinely updated, unless it is necessary for the purpose for which it is to be used or disclosed.

Data Security

AIS will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. AIS will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under AIS Privacy Protection Principles.

a. Documenting security and storage.
   AIS will document security and storage requirements for all personal information for which it is responsible, including physical and logical controls. In developing security and storage requirements, AIS will take into consideration the sensitivity of the information, its form and volume, its frequency of use and retention period, the circumstances of its use and storage and any legal or regulatory requirements.
b. Electronic Systems.
   Where personal information is held on electronic systems AIS will implement reasonable measures to protect the security of that information and limit access to that required for the provision of services or fulfilling AIS's legitimate functions.
c. Orderly storage.
   Personal information will be stored in an orderly fashion in order to facilitate awareness of its existence and access thereto.

d. Personal Information retention and disposal requirements.
AIS will take reasonable measures to ensure the retention and disposal requirements for all personal information for which it is responsible, taking into consideration the sensitivity of the information, its form, the circumstances of its use and any legal or regulatory requirements.

e. Secure disposal.
When personal information is no longer required to be kept, such information will be destroyed or made anonymous in a controlled and secure manner in order to prevent any unauthorised persons having access to that information.

f. Information subject to complaint, inquiry or legal process.
Personal information, which is the subject of complaint, inquiry or legal process, will not be destroyed until the resolution of that process. Staff, agents and contractors should adopt a "clean desk" policy in relation to personal information. That is, when not being used by staff, documents containing personal information should be put away or stored in a manner, which prevents it being viewed by others.

Openness

AIS will set out in a document clearly expressed policies on its management of personal information. AIS will make the document available to anyone who asks for it.

On request by an individual, AIS will take reasonable steps to let the individual know, generally, what sort of personal information it holds, for what purposes, and how it collects, uses, and discloses that information.

The Company Secretary is responsible for ensuring that AIS's Privacy Protection Principles and procedures as set out in this document remain appropriate and that AIS operates in compliance with those principles and procedures. Explanatory information about AIS's Privacy Protection principles and their application will be available to the public.

Community awareness

In order to ensure awareness in the general community, AIS will make freely available, upon request, details of its Privacy Protection Principles together with general details of the types of personal information held, its use, disclosure and retention. AIS will provide facilities to enable individuals to make enquires and to register their comments about the Privacy Protection Principles.

Compliance obligation

Anyone handling personal information for which AIS, or an Australian subsidiary in which AIS has a controlling interest, is responsible, whether employee, agent or contractor, is expected to act in accordance with the Principles and procedures set out in this document.

Internal compliance program

AIS will maintain a compliance program to ensure that it's Privacy Protection Principles are applied to all personal information and privacy-sensitive activities and to encourage a culture of protecting personal information.

The objectives of the compliance program are to:

a. Educate employees, contractors and agents about the Company's principles, procedures and related procedures;
b. Establish and maintain supervisory and system controls that are commensurate with the sensitivity of the information to be protected;
c. Incorporate these principles in privacy and customer service procedures;
d. Ensure that an assessment of privacy implications is an integral part of the company's product and service development programs;
e. Require agents and contractors to comply with these principles.

Access and Correction

If AIS holds personal information about an individual, it will provide the individual with access to the information on request by the individual, in a form or manner suitable to the individual's reasonable needs, except to the extent that:

a. in the case of personal information other than health information – providing access would pose a serious and imminent threat to the life or health of any individual;
b. in the case of health information – providing access would pose a serious threat to the life or health of any individual;
c. providing access would have an unreasonable impact upon the privacy of other individuals;
d. the request for access is frivolous or vexatious;
e. the information relates to existing or anticipated legal proceedings between AIS and the individual, and the information would not be accessible by the process of discovery in those proceedings;
f. providing access would reveal the intentions of AIS in relation to negotiations with the individual in such a way as to prejudice those negotiations;
g. providing access would be unlawful;
h. denying access is required or authorised by or under law;
i. providing access would be likely to prejudice an investigation of possible unlawful activity;
j. providing access would be likely to prejudice:

i. the prevention, detection, investigation, prosecution, punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
ii. the enforcement of laws relating to the confiscation of the proceeds of crime;
iii. the protection of the public revenue;
iv. the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
v. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders by or on behalf of an enforcement body;

a. an enforcement body performing a lawful security function asks AIS not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

However, where providing access would reveal evaluative information generated within AIS in connection with a commercially sensitive decision-making process, AIS may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

If AIS has given an individual an explanation under paragraph above, and the individual believes that direct access to the evaluative information is necessary to provide a reasonable explanation of the reasons for the decision, AIS will, at the request of the individual, undertake a review of the decision not to provide access. Personnel other than the original decision-maker will undertake the review.

If AIS is not required to provide the individual with access to the information because of one or more of paragraphs above (a) - (k), AIS will, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

If AIS levies charges for providing access to personal information, those charges:

a. will not be excessive, sufficient to recover time and materials costs; and
b. will not apply to lodging a request for access.

If AIS holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, AIS will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

If the individual and AIS disagree about whether the information is accurate, complete and up-to-date, and the individual asks AIS to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, AIS will take reasonable steps to do so.

AIS will provide reasons for denial of access or a refusal to correct personal information.

Consistency with the Freedom of Information Act 1982 ("FOI Act")

None of the Procedures set out here are to be read as being inconsistent with the operation of the FOI Act.

Access to personal information

AIS has developed a Procedure for handling requests for access to and correction of personal information under the Privacy Act (see reference section). Individuals are entitled to inquire whether AIS holds personal information concerning them and if so to be advised of its use and disclosure and to obtain a copy or transcript of any relevant document.

Identifiers

Except as specifically authorised under the Privacy Act, AIS will not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

a. a Federal agency;
b. a Federal agent of, a Federal agency acting in its capacity as agent;

c. a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

AIS will not use or disclose an identifier assigned to an individual by a Federal agency (or by an agent, or contracted service provider mentioned above unless:

a. the use of disclosure is necessary for AIS to fulfil its obligations to the agency;
b. one or more of paragraphs Use & Disclosure (e) - (h) apply to the use or disclosure,
c. or the use or disclosure is permitted under the regulations to the Privacy Act.

A customer may be required to establish their identity by means of a government assigned identifier but AIS will not insist on the customer providing a particular government assigned identifier (unless required to do so by law) nor will it use such identifier to organise personal information it holds and match it with other personal information organised by reference to the same identifier. However, an individual's name or ABN is not such an identifier.

Anonymity

Wherever it is lawful and practicable, individuals will have the option of not identifying themselves when entering transactions with AIS. However, in most cases it will not be practicable for AIS to provide pre- and post-paid services without requiring customer identification.

In most circumstances, AIS will require identification from its customers for practical and/or legal reasons. If there are no such reasons in a particular situation, AIS will give a customer the option of operating anonymously in their dealings with AIS.

Trans-border Data Flows

AIS will transfer personal information about an individual to someone (other than AIS or the individual) who is in a foreign country only if:

a. AIS reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to AIS's Privacy Protection Principles;
b. the individual consents to the transfer;
c. the transfer is necessary for the performance of a contract between the individual and AIS, or for the implementation of pre-contractual measures taken in response to the individual's request;
d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between AIS and a third party;
e. all of the following apply:

    i. the transfer is for the benefit of the individual;
    ii. it is not practicable to obtain the consent of the individual to that transfer;
    iii. if it were practicable to obtain such consent, the individual would be likely to give it;

iv. AIS has taken reasonable steps to ensure that the information, which it has transferred, will not be held, used or disclosed by the recipient of the information inconsistently with AIS's Privacy Protection Principles.

Sensitive Information

AIS will not collect Sensitive Information about an individual unless:

a. the individual has consented; or
b. the collection is required by law; or
c. the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
    i. is physically or legally incapable of giving consent to the collection; or
    ii. physically cannot communicate consent to the collection; or
    iii. the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
d. AIS may however collect health information about an individual if:
    i. the information is necessary to provide a health service to the individual; and
    ii. the information is collected as required by law (other than the Privacy Act); or
    iii. in accordance with rules established by competent health or
    iv. medical bodies that deal with obligations of professional confidentiality which bind AIS.
e. AIS may collect health information about an individual if the collection is necessary for any of the following purposes:
    i. research relevant to public health or public safety;
    ii. the compilation or analysis of statistics relevant to public health or public safety;
    iii. the management, funding or monitoring of a health service;
    iv. that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained;
    v. it is impracticable for AIS to seek the individual's consent to the collection;
    vi. the information is collected as required by law (other than the Privacy Act);
    vii. in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind AIS; or
    viii. in accordance with guidelines approved by the Privacy Commissioner under section 95A of the Privacy Act.

If AIS collects health information about an individual, AIS will take reasonable steps to permanently de-identify the information before AIS discloses it.

Non Discriminatory

AIS will not collect, use or disclose information about an individual's:

a. political, social or religious beliefs or affiliations;
b. race, ethnic origins or national origins; or

c. sexual preferences or practices;

unless the collection or use is in accordance with this procedure.

Private lives

AIS respects the right of individuals to the privacy of their personal lives and requires all employees, agents and contractors working on behalf of AIS to respect this basic right. AIS emphasises to its staff that information such as records of numbers called, calling patterns, internet sites visited and some customers (and third parties) may also regard geographical location of parties at the time of calls as sensitive information.

Working environment

AIS will provide a working environment which is commensurate with the company's privacy principles and privacy protection procedures and which provides an appropriate degree of personal privacy for its employees and contractors.

Surveillance

Surveillance of customers, employees or contractors will only be undertaken by lawful means and in accordance with this and any other applicable company procedure. All proposals to conduct surveillance will require the prior written approval of the Company Secretary and Managing Director.

Access to AIS's business information

AIS reserves the right to access its business records (including call records for business phones) created by employees, agents or contractors and to investigate any suspected improper conduct such as suspected fraud, theft or other illegal act or suspected breach of Company Procedures and Guidelines.

Any such investigation will only be conducted in compliance with relevant legislation and Company Procedures and Guidelines. Any personal information disclosed to third parties in the course of such an investigation will be restricted to that appropriate in the circumstances.

Old criminal convictions

AIS will comply with the provisions of the Crimes Act 1914 which apply safeguards to the collection of information about old, minor and spent criminal convictions.

Privacy of Network Communications

When installing, operating, or maintaining its network, AIS will take whatever measures are practicable, or are required by law, to ensure the privacy of communications passing over its network.

Interception (Monitoring and Recording)

Interception of a communication during the course of its passage across the network is prohibited unless it is necessary for the effective performance of functions or activities relating to:

a. the installation of any line or equipment used in connection with the network; or

b. the operation or maintenance of the network; or
c. the identifying or tracing of a person suspected of having contravened a provision of Part VIIB of the Crimes Act 1914; or
d. interception requested by law enforcement and security agencies will only be undertaken on production of a lawful warrant and where AIS is satisfied that the warrant has been issued in accordance with the requirements of the Telecommunications (Interception) Act 1979;
e. recording will only be undertaken where aural/visual monitoring is not suitable for the purpose and voice recording will only be undertaken where authorised by the customer or by law.

Interception will only be undertaken in accordance with company procedures. Only staff who have received instruction on the appropriate monitoring and recording procedures and who are aware of their responsibilities for the protection of customer privacy and confidentiality will be permitted to undertake monitoring functions.

Participant Monitoring

Participant monitoring may be undertaken for the purposes of improving the quality of service to customers and the training of staff, or where there is a specific operational, security or technical reason to do so. Customer consent will be obtained prior to undertaking participant monitoring unless it is not practicable to do so, such as in the case of calls which are typically of very short duration.

Privacy expectations

AIS will provide services with a privacy standard which is commensurate with community expectations and which enables individual customers to choose a higher degree of privacy protection where practicable.

Privacy implications of change

The privacy impact arising from the introduction of the new services or products will be balanced against their benefit to the general community and will take into consideration the extent, means and cost by which privacy concerns can be mitigated. Where practicable, AIS will provide customers with the ability to choose between differing degrees of privacy protection.

Education and choice

In order that customers may make an informed choice as to their usage of new services or products, where appropriate AIS will advise customers of the privacy implications of those services. Where practicable, and where to do so would not undermine commercially sensitive material, AIS will respond to queries concerning any implications for privacy protection of existing and new services and make publicly available information about any implications for privacy protection in relation to those services.

Compliance Audit

AIS will maintain an internal compliance audit program to ensure its Privacy Protection Principles and policies remain appropriate and that AIS operates in compliance with those Principles and policies.

The Telecommunications Act

Part 13 of The Telecommunications Act prohibits employees, contractors and service providers to AIS from using or disclosing customer information obtained because of being an employee, contractor or service provider, except as permitted by Part 13 of The Telecommunications Act. In this regard customer information is defined as:

a. the contents or substance of a communication;
b. telecommunication services supplied or to be supplied by a carrier or service provider to a person; and
c. the affairs or personal particulars of a person.

Breach of the Telecommunications Act is a criminal offence. Further duties and obligations are imposed on AIS through the Telecommunications Act and the licensing regime. These principally address the transfer of information between AIS, other carriers and the Government.

ACIF Privacy Code

ACIF has produced an industry code of practice on Protection of Personal Information of Customers of Telecommunications Providers which is registered by the ACA.

The Telecommunications (Interception) Act 1979

The Telecommunications (Interception) Act 1979 expressly prohibits the interception of communication passing over a telecommunications system, except in certain limited circumstances, and regulates the subsequent use of any information obtained as a result of that interception. The circumstances in which the Act permits the interception of communications includes interception by employees of a carrier in the course of their duties in connection with the installation, operation or maintenance of a telecommunications system.

The Privacy Act

AIS's responsibilities under the Privacy Act relate to the handling of personal information, sensitive information, credit information and Tax File Numbers, as follows:

a. Personal information and sensitive information

   AIS is obliged to comply with the National Privacy Principles on the collection, holding, use, correction, disclosure or transfer of personal information and sensitive information as detailed in Schedule 3 of the Privacy Act.

b. Credit information

   AIS is obliged to comply with the operation of the credit information provisions of Part IIIA of the Privacy Act, and in particular the Credit Reporting Code of Conduct which addresses the collection, use and disclosure of credit information.

c. Tax File Numbers

AIS is obliged to comply with the Tax File Number provisions of the Privacy Act, and in particular the Tax File Number Guidelines. These address the collection, use, security, disclosure and disposal of Tax File Number information.

The FOI Act

AIS is subject to the FOI Act, which provides an applicant with the right to seek access to records concerning themselves and in certain circumstances to seek amendment to those records.

The Crimes Act 1914

Under the terms of the Crimes Act 1914, AIS is obliged to comply with the safeguards applying to the collection of information about old, minor, spent criminal convictions.

The Archives Act 1983

AIS is subject to the Archives Act 1983.

Definitions

In this Policy, the following words have these meanings unless the contrary intention appears:

ACMA means the Australian Communications and Media Authority.

ACIF means the Australian Communications Industry Forum.

ACIF Privacy Code means the industry code entitled 'Protection of Personal Information of Telecommunications Providers' (ACIF C523 December 1999) registered by the ACMA pursuant to section 117 of the Telecommunications Act, as amended from time to time.

ASIO means the Australian Security Intelligence Organisation.

Authorised Officer means in relation to an Enforcement Agency, the meaning given to that term by section 282(10) of the Telecommunications Act.

Carrier has the meaning given by the Telecommunications Act.

Carriage Service Provider has the meaning given by the Telecommunications Act.

Collection means the act of gathering, acquiring or obtaining personal information from any source, including from third parties, by any means. Does not include the receipt of unsolicited (that is, unexpected) information.

Consent means the free and informed agreement with what is being done or proposed. **Consent** can be either express or implied.

Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of AIS. Implied consent arises where consent may be reasonably inferred from the action or inaction of the individual.

Disclosure means making personal information available to others outside AIS, other than to the subject of the information. Disclosure includes publication of personal information through any medium.

Enforcement Agency means the meaning given to that term by section 282(10) of the Telecommunications Act.

FOI Act means the Freedom of Information Act 1982, as amended from time to time.

Generally Available Publication means a publication (whether in paper or electronic form) that is generally available to members of the public.

Identifier includes a number assigned by an organisation to an individual to identify uniquely that individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an identifier.

Individual means a natural person.

Monitoring means the listening to, reading or recording of a communication during the course of its passage over a telecommunication system.

Participant monitoring means the listening to, reading or recording of, a communication during the course of its passage over a telecommunication system by a party to that communication and by using equipment forming part of the service.

Personal Information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Privacy Act means the Privacy Act 1988, as amended from time to time.

Recording means the recording of a communication passing over a telecommunications system on magnetic tape or other medium.

Sensitive Information means information or an opinion about an individual's:

a. racial or ethnic origin; or
b. political opinions; or
c. membership of a political association; or
d. religious beliefs or affiliations; or
e. philosophical beliefs; or
f. membership of a professional or trade;
g. association; or

h. membership of a trade union; or
i. sexual preferences or practices; or
j. criminal record;
k. that is also personal information; or
l. health information about an individual.

Seriously Improper Conduct includes corruption, a serious abuse of power, a serious dereliction of duty, or any other seriously reprehensible behaviour.

Surveillance means the systematic observance of a person's behaviour, communication or personal information.

Telecommunication Act means the Telecommunications Act 1997, as amended from time to time.

Third Party in relation to personal information, means any organisation or individual other than AIS holding the information and the individual who is the subject of the information.

Use means the treatment and handling of personal information within AIS.