Mega International Commercial Bank Co. Ltd
Australia Branch

Privacy Policy

Approved By	AMC	SOOA	Approve No
Date of approval (V 1.0)	28 July 2011	29 August 2011	01714
Date of approval (V 1.1)	24 July 2012	22 August 2012	01772
Date of approval (V 1.2)	13 June 2013	30 July 2013	1695

Version 1.2

Policy Owner The Head of Risk and Compliance

Approved Australian Management Committee (AMC)

Senior Officer Outside Australia (SOOA)

Document Version Control

Version ID	Date	Author	Remarks
Draft	1 July 2011		Document Creation
Draft	10 July 2012		Document Update
Draft	..June 2013		Document Update

Document Review and Approval

Name	Position	Reviewer/Approver	Signature(if Required)
Mr Shiu	SOOA	Approver	
AMC		Approver	
AT	Country Head	Reviewer	
SH	HRC	Reviewer	

Contents

Introduction

The Privacy Amendment (Private Sector) Act 2000 (Act) commenced on 21 December 2001 and extended the Privacy Act 1988 to the private section by introducing 10 National Privacy Principles (NPPs). The Privacy Act 1988 has been further amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (the Reform Act). The Reform Act includes a set of 13 new, harmonised, privacy principles for both the private and public sector, called the Australian Privacy Principles (APPs). The 13 APPs will replace the NPPs from 12 March 2014.

The NPPs and APPs (The Principles) represent the minimum standards of privacy protection policy that must be adopted and regulate the collection, security, storage, use and disclosure of personal information for organisations.

Applicability

The Principles apply to "organisations". Mega International Commercial Bank Co., Ltd （Mega ICBC）holds an Australian Services Licence and therefore is identified as an "organisation" for the purposes of thePrinciples.

Personal and Sensitive Information

The Act protects personal information. This is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information. Personal information includes names, age, gender, contact details and financial information. It also includes credit card details, information on credit history, credit reports from credit reporting agencies, information gathered on websites and mobile telephone numbers linked to user names and mailing lists.

There is extra protection for sensitive information. Sensitive information includes information about a person's racial or ethnic origin, political or religious belief, philosophical beliefs, membership of professional or trade associations or unions, sexual practices and criminal record. It also includes health and genetic information.

The Principles and Policy Codes

Mega ICBC is bound either by the Principles or a registered policy code. The Principles set out the minimum standards required for the handling of personal information by organisations. They set the baseline standards for privacy protection. Mega ICBC complies with the Principles. Mega ICBC may in its absolute discretion adopt any other approved privacy policy in the future.

Australian Privacy Principles

Mega ICBC will be bound by the 13 APPs from 12 March 2014. The APPs will replace the NPPs and are attached at Appendix B.

The Ten National Privacy Principles

The NPPs mainly apply to personal information collected on or after 21 December 2001. However organisations such as Mega ICBC will have some obligations under the NPPs with respect to the:

- Accuracy and completeness;
- Security and disposal;
- Policies for management;
- Access and correction; and

- Transborder movement;

of personal information they hold after 21 December 2001, even if the information was collected before the commencement of the Act.

The following are guidelines to the NPPs that are to be followed and adhered to by Mega ICBC. These are not a substitute for the complete NPPs which represent the minimum standard of privacy protection.

NPP1 – Collection

Mega ICBC must not collect personal information unless the information is necessary for one or more of its functions or activities. It is not acceptable for Mega ICBC to collect information simply because it would like to have, or it might need to have, that information some time in the future.

Information must be collected by lawful and fair means and not in an unreasonably intrusive way. If reasonable and practicable to do so Mega ICBC should always endeavour to collect personal information directly from the person concerned.

Mega ICBC must take reasonable steps to inform the person about their identity and contact, the purpose of collection, and the person's right to access the information after it has been collected. This applies even if the information is collected from someone else.

Most of personal information will be collected from the Application Form provided to a customer. A statement as to the information collection and its purpose is included on each Application Form. A Privacy and Spam Statement (see Appendix A) is also included with the Application Form and provided to all prospective customers in order to provide information in relation to our Privacy Policies.

NPP2 – Use and disclosure

Mega ICBC must not use or disclose personal information about a person for a purpose other than the primary purpose of collection unless:

- The secondary purpose is related to the primary purpose of collection and the individual would reasonably expect Mega ICBC to use or disclose the information in that way; or
- The individual has consented to the use or disclosure; or
- It uses the information in a particular way for direct marketing subject to certain conditions; and
- The use or disclosure is otherwise authorised by law.

For Mega ICBC, the sole use of the information is for further communications to customers, and for advising them of the availability of future products.

NPP3 – Data quality

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

NPP4 – Data security

Mega ICBC must take reasonable steps to protect the personal information it holds from misuse or loss and from unauthorised access, modification or disclosure.

It must also destroy or de-identify the information if it is no longer needed.

NPP5 – Openness

Mega ICBC's expressed policies on the management of personal information are set out in Appendix A – Privacy and Spam Statement. The Statement will be made available to all prospective customers and to anyone who requests it.

If requested, Mega ICBC must take reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses, and discloses that information.

NPP6 – Access and correction

Mega ICBC must provide individuals with access to and a copy of their personal information on request. This includes information collected from third parties, information received unsolicited and subsequently kept in records held, and opinions recorded about an individual.

Mega ICBC must also incorporate processes for the correction of information on the request of individual or if there is some disagreement as to the correction, allow a statement to be associated with the information noting that the individual desires a correction.

Mega ICBC may choose to charge for access to personal information. Those charges must not be excessive and must not apply to lodging a request for access.

NPP7 – Identifiers

An identifier is a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. An individual's name or ABN is not an identifier.

Mega ICBC is prohibited from adopting as its own identifier of an individual an identifier that has been assigned by a government agency, or a contracted service provider for a Commonwealth contract such as Tax File Numbers (TFNS), Medicare and pension numbers.

NPP8 – Anonymity

Whenever it is lawful and practicable, Mega ICBC should give individual the option of not identifying themselves hen entering into transaction with Mega ICBC.

NPP9 – Transborder data flows

Mega ICBC may only transfer personal information about an individual to someone in a foreign country if:

It reasonably believes that the recipient of the information is subject to a law, binding contract that is substantially similar to Australia's National Privacy Principles;

- The individual consents to the transfer; or
- The transfer is necessary for the performance of a contract involving the individual.

NPP10 – Sensitive and health information

Mega ICBC must not collect sensitive information about an individual unless:

- The individual has consented;
- The collection is required by law;
- The collection is necessary to prevent or lessen a serious or imminent threat to life or health; or
- The collection is necessary for establishment, exercise or defence of a legal or equitable claim.

Appointment of Privacy Officer

SOOA may at its absolute discretion appoint or employ any person to be the Privacy Officer of the company. The Privacy Officer would be the first point of contact in Mega ICBC when privacy issues arise either internally or externally.

Until determined otherwise by SOOA, the Head of Risk and Compliance is appointed as the Privacy Officer.

The Privacy Officer is responsible for:

- Developing and implementing a privacy policy that suits the Mega ICBC's business and complies with the law;
- Ensuring that Mega ICBC's privacy policy and procedures are fully implemented and working effectively; and
- Reporting to SOOA any breach of the privacy policy.

Complaints

An individual may make a complaint in writing by either asking to complete our complaint form detailing the problem or sending us a letter, email or facsimile. If they do not wish to make the complaint in writing, they may make the complaint in person, or we will take down details of their complaint over the telephone.

Mega ICBC will investigate, address and if necessary escalate the complaint as required under our Privacy Policy.

Policy Review

The Risk and Compliance department will review this policy annually and will update it, when required, between review dates to reflect legislative or regulatory changes.

This policy is supported by further procedures and operational arrangements. If you have any questions regarding this policy, then please contact the Head of Risk and Compliance.

The policy will be communicated to all new members of staff by the Risk and Compliance department during induction training sessions.

A breach of this policy will be considered as professional misconduct and will be liable for disciplinary penalties. This could potentially include immediate dismissal and legal action. (Refer to Mega ICBC Risk Event and Breach Escalation Policy)

Appendix A. Privacy and Spam Statement

Privacy and Spam Statement 隱私同意書

This Statement explains how Mega International Commercial Bank Co., Ltd ("we/us/our") collects, uses and discloses Personal Information. For the purposes of this Privacy and Spam Statement, "Personal Information" is information which may be used to identify an individual, including name, age, gender, contact details and financial information such as credit history. By law, we are required to collect and store this information in accordance with prudent risk management, banking and anti-money laundering and counter terrorism financing legislation.

As well as dealing with our collection, use and disclosure of Personal Information, this Statement requests your consent to us sending you information about products and services, including by way of commercial electronic messages. Where you sign this Statement, you are providing your consent to the disclosures and contacts outlined in this Statement.

Purposes for which we collect and use Personal Information

(i) We may collect your Personal Information to allow us to assess and process your application for a product or facility, as well as to establish, provide and administer any product or facility we have agreed to provide to you.

(ii) We may also use your Personal Information to allow us to:

- comply with relevant state and federal legislative and regulatory requirements (such as customer identification);
- consider any other application you may make to us, including applications for commercial credit;
- perform our required business administration, including account keeping, risk management, record keeping, archiving, systems development and testing, credit scoring, fraud prevention and staff training;
- manage our rights and obligations in relation to external payment systems;
- conduct market or customer satisfaction research;
- develop, establish and administer alliances and other arrangements (including rewards programs) with other organisations in relation to the promotion, administration and use of our respective products and services;
- develop and identify products and services that may interest you; and
- tell you about products and services (unless you request that we not do so).

(iii) You agree that, in assessing an application for credit or in assessing whether to accept you as a guarantor to an application for credit, we may obtain a credit report about you or personal information about you in a credit report, from a credit reporting agency or organisation or a credit provider ~~and use it in~~ for the purpose of assessing whether to accept you as a borrower or guarantor.

(iv) If we do not collect Personal Information about you, we may not be able to provide you with our products or services.

(v) If you provide Personal Information to us about someone else, you agree that you will show them a copy of this Privacy and Spam Statement, to allow them to understand the manner in which their Personal Information may be used or disclosed by us in connection with your dealings with us.

Disclosure of Personal Information

(i) You agree and acknowledge that we may disclose Personal Information we have collected about you to:

- credit reporting agencies for the purpose of obtaining a credit report or to allow the credit reporting agency to create or maintain a credit information file containing information about you;
- any credit provider for any purpose you have agreed to;
- our agents, contractors, service providers and external advisers;
- your agents and contractors, including your finance broker, builder, settlement agent and your legal or financial adviser;
- your executor, administrator, trustee, guardian or attorney;
- your referees;

- regulatory bodies, government agencies, law enforcement bodies and courts;
- debt collection agencies;
- any person or organisation who introduces you to us;
- anyone supplying goods or services to you in connection with a rewards program associated with a loan or facility you have (or have applied for) with us;
- other financial institutions and our related companies;
- other organisations with whom we have alliances or arrangements (including rewards programs) for the purpose of promoting our respective products and services (and any agents used by us and our business partners in administering such an arrangement or alliance);
- your franchisor (if applicable);
- external payment systems operators;
- any mortgage insurer used by us and reinsurer of such mortgage insurer;
- our insurers or prospective insurers and their underwriters;
- an intending guarantor, to enable that person to consider whether or not to act as guarantor, or offer property as security, for a loan you have (or have applied for) with us;
- your co-borrowers, sureties, guarantors and co-guarantors and prospective co-borrowers, sureties, guarantors and co-guarantors;
- any person considering purchasing your loan, guarantee or security, that person's advisers, persons involved in assessing the risks and funding of the purchase and, after purchase, the purchaser and any manager on an ongoing basis;
- any person to the extent necessary, in our view, in order to carry out any instruction you give us; and
- other organisations (including our related bodies corporate) and their agents for the marketing of their products and services (unless you request that we not do so).

(ii) You agree that we may make such disclosures even if the disclosure is to an organisation overseas which is not subject to the privacy obligations which are equivalent to those which apply to us, and we will not remain liable for the information once it is disclosed overseas.

(iii) We operate throughout Australia and in a number of countries overseas. As a result, you agree that some of these uses and disclosures may occur interstate or outside Australia. Please contact us if you wish for a list of the countries in which we operate.

Gaining access to and correction of your Personal Information

You may seek to gain access to your Personal Information held by us at any time by contacting one of our branches. We may charge an administration fee to allow access to this information.

If we are satisfied that your personal information held by us is inaccurate, incomplete or out of date then we will correct this. If you wish to request us to correct your information, please inform us as soon as practicable so that this can be updated. You may be required to provide new forms of evidence to support any requested changes to your Personal Information.

We will only deny you access to or refuse a correction of your Personal Information where we have a reason to do so or where required by law. In these circumstances, we will provide you with reasons (where possible) for denying your request. This may be because the information that you have requested access to is commercially sensitive, or we are prohibited or permitted to do so by law.

Complaints

If a matter is not or cannot be resolved immediately to your satisfaction and to our satisfaction, you may make a complaint in writing by either asking to complete our complaint form detailing the problem or sending us a letter, email or facsimile. If you do not wish to make the complaint in writing, you may make the complaint in person at one of our branches, or we will take down details of your complaint over the telephone. We will investigate and address your complaint within 10 Business Days. If you are not satisfied with the outcome, we will escalate your complaint internally and will inform you of the result of the escalation of your complaint.

If you are not satisfied with the outcome of the above process you may contact the Financial Services Ombudsman by completing and sending FOS a Dispute Form (available at www.fos.org.au) or by calling the Financial Services Ombudsman at 1300 78 08 08.

Receiving commercial electronic messages

(i) You consent to us sending commercial electronic messages, including messages about our products and services and the products and services of any third party that we think may be of interest to you, to each electronic address which you have provided to us. You warrant that you have authority either as or on behalf of the relevant electronic account holder to provide this consent.

(ii) In respect of each electronic address, you agree that until you provide written notice to withdraw your consent in respect of that electronic address or use an unsubscribe facility included within a commercial electronic message sent to that electronic address (to withdraw your consent), we may continue to send commercial electronic messages to that electronic address.

(iii) You may, at any time, ask us not to mail, telephone or send you information about products and services and not to disclose your Personal Information to any other organisations for that purpose. You may do this by contacting one of our branches.

For more information about the way in which we collect and use your Personal Information, please contact Mega International Commercial Bank Co., Ltd.

X

Name of 1st Applicant 第一申請人姓名		**Date 日期**	

X

Name of 2nd Applicant 第二申請人姓名		**Date 日期**	

Appendix B

The Thirteen Australian Privacy Principles

The APPs mainly apply to personal information collected on or after 21 December 2001. However organisations such as Mega ICBC will have some obligations under the APPs with respect to the:

- Accuracy and completeness;
- Security and disposal;
- Policies for management;
- Access and correction; and
- Transborder movement;

of personal information they hold after 21 December 2001, even if the information was collected before the commencement of the Act.

The following are guidelines to the APPs that are to be followed and adhered to by Mega ICBC.

APP1 – Open and transparent management of personal information

The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Mega ICBC is required to have a clearly expressed and up to date policy about the management of personal information which contains the following information:

- The kinds of personal information that we collect and hold and how we do this;
- The purposes for which we collect, hold, use and disclose personal information;
- How an individual may access personal information about the individual held by us and seek the correction of such information;
- How an individual may complain about a breach of the APPs and how we will deal with that complaint; and
- Whether we are likely to disclose personal information to overseas recipients and those countries where the recipients are located (where practical to specify).

Mega ICBC's expressed policies on the management of personal information are set out in Appendix **A – Privacy and Spam Statement.** The Statement is made available to all prospective customers and to anyone who requests it free of charge and in the form that the individual or body requests it.

If requested, Mega ICBC must take reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses, and discloses that information.

APP2 – Anonymity and pseudonymity

Individuals must have the option of not identifying themselves or of using a pseudonym, when dealing with Mega ICBC in relation to a particular matter.

This does not apply where Mega ICBC is required or authorised by or under an Australian law (for example the AML/CTF Act), or a court/tribunal order, to deal with individuals who have identified themselves or where it is impracticable for us to do so.

APP3 – Collection of solicited personal information

Mega ICBC cannot collect personal information from an individual unless that information is reasonably necessary for one of our functions or activities. It is not acceptable for us to collect information simply because we would like to have, or might need to have, that information at some time in the future.

Information must be collected by lawful and fair means and not in an unreasonably intrusive way. If reasonable and practicable to do so, we should always endeavour to collect personal information directly from the person concerned.

Mega ICBC must not collect sensitive information about an individual unless:

- the individual has consented and the information is reasonable necessary for one or more of Mega ICBC's functions or activities; or
- the collection is required or authorised by or under an Australian law or a court/tribunal order; or
- we reasonably believe that collection is necessary to lessen or prevent a serious threat to the life, health or safety of an individual and it is unreasonable or impracticable to obtain the individual's consent to the collection; or
- we have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to Mega ICBC's functions or activities has been, is being or may be engaged in, and we reasonably believe that the collection is necessary for us to take appropriate action in relation to the matter; or
- we reasonably believe that the collection is reasonably necessary to assist the location of a person who has been reported as missing.

Most personal information will be collected from the Application Form provided to a customer. A statement as to the information collection and its purpose is included on each Application Form. A Privacy and Spam Statement (see Appendix A) is also included with the Application Form and provided to all prospective customers in order to provide information in relation to our Privacy Policies. The Privacy and Spam statement is required to be signed by the customer and returned to Mega ICBC.

APP4 – Dealing with unsolicited personal information

Unsolicited personal information (personal information we receive but did not request) must be given the same protection by Mega ICBC as solicited personal information.

Where Mega ICBC receives unsolicited personal information:

- we must determine whether it could have collected it under APP3
- if the information could have been collected, then APPs 5 to 13 will apply to the information

- if we decide we couldn't have collected the information, then we must destroy or de-identify the information as soon as practicable, but only if lawful and reasonable to do so, and only if the information is not contained in a commonwealth record.

APP5 – Notification of the collection of personal information

Mega ICBC must take reasonable steps to ensure that individuals are aware of the following at or before the time of collecting the personal information:

- Mega ICBC's identity and contact details;
- if collection is required or authorised under the law, then fact and details of requirement;
- the purpose of collection;
- consequences of non-collection;
- the organisations to which the personal information of that kind is usually disclosed;
- the person's right to access the information after it has been collected and seek correction if necessary ;
- how the person may complain about a breach of the APPs and how Mega ICBC will deal with such a complaint; and
- whether Mega ICBC is likely to disclose the information to overseas recipients and if so the countries in which the recipients are likely to be located.

If Mega ICBC collects the personal information from someone other than the individual, then we need to take reasonable steps to ensure the individual is aware that we have collected the information and the circumstances of the collection.

The Mega ICBC Privacy and Spam Statement (Appendix A) contains all the above required information and should be provided to all prospective customers. The Privacy and Spam Statement is required to be signed by the customer and returned to Mega ICBC.

APP6 –Use or disclosure of personal information

Mega ICBC must not use or disclose personal information about a person for a purpose other than the primary purpose of collection unless:

- The secondary purpose is related to the primary purpose of collection and the individual would reasonably expect us to use or disclose the information in that way; or
- The individual has consented to the use or disclosure; or
- The use or disclosure is authorised under Australian law or a court/tribunal order; or
- It is necessary to lessen or prevent a serious threat to the life, health or safety of an individual and it is unreasonable or impracticable to obtain the individual's consent to the collection; or
- It is necessary for us to take action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to Mega ICBC's functions or activities; or
- we reasonably believe it is necessary to assist the location of a person who has been reported as missing; or
- we reasonably believe it is necessary for enforcement related activities conducted by an enforcement body.

For Mega ICBC, the sole use of the information is for further communications to customers, and for advising them of the availability of future products. The Mega ICBC Privacy and Spam Statement (Appendix A) provides information to customers regarding disclosure of their personal information and is required to be signed by the customer and returned to Mega ICBC.

APP7 –Direct Marketing

Mega ICBC may only use or disclose personal information it has collected from an individual (other than sensitive information) for direct marketing purposes if the individual would reasonably expect that their personal information would be used or disclosed for direct marketing. In addition, we need to have provided a simple means by which the individual can request not to receive direct marketing and not have received such a request.

Where an individual would not reasonably expect their personal information (other than sensitive information) to be used for direct marketing, or the information has been collected from a third party, Mega ICBC may only use or disclose the personal information for direct marketing if:

- the individual has consented to the use or disclosure for this purpose, or it is impracticable to seek this consent; and
- we have provided a simple means by which the individual can opt out of direct marketing and the individual has not opted out; and
- in each direct marketing communication the organisation must include a prominent statement telling the individual that he or she may request to no long receive direct marketing, and no request is made.

Mega ICBC is required to obtain the consent of the individual before using or disclosing sensitive information for the purpose of direct marketing.

Individuals have the right to contact Mega ICBC to request the following and we need to comply with the requests in a reasonable time and free of charge:

- request not to receive direct marketing communications from us;
- request that we do not disclose their personal information to other organisations for the purpose of direct marketing; or
- request that we provide our source for the individual's personal information (we do not need to comply with this if it is unreasonable or impracticable).

The Mega ICBC Privacy and Spam Statement (Appendix A) is required to be signed by the customer and states that:

- we may disclose personal information of a customer to other organisations and their agents for the marketing of their products and services, unless a customer requests that we do not do so; and
- a customer may, at any time, ask us not to mail, telephone or send them information about products and services and not to disclose their personal information to other organisations for that purpose. A customer may do this by contacting one of our branches.

APP8 –Cross-border disclosure of personal information

If Mega ICBC in Australia discloses personal information about an individual to an overseas recipient (i.e. a person not in Australia or an external territory) who is not the same entity as Mega ICBC, then under APP 8.1 we have to ensure that the overseas recipient doesn't breach the APPs.

Mega ICBC may then only transfer personal information about an individual to a person in a foreign country if:

- we reasonably believes that the recipient of the information is subject to a law or binding scheme in a way that, overall, is at least substantially similar to the way the APPs protect the information; and there are mechanisms available to the individual to enforce that protection or scheme; or
- the individual consents to cross-border disclosure, after we inform them that APP 8.1 will no longer apply if they give their consent; or
- where the cross border disclosure is required or authorised by or under an Australian law, or a court order; or
- where we reasonably believe the disclosure to be necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety; or
- where we reasonably believe that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to our functions or activities; or
- where we reasonably believe that the disclosure is necessary to assist any APP entity, body or person to locate a person who has been reported as missing.

The Mega ICBC Australia Branch Privacy and Spam Statement (Appendix A) is required to be signed by customers and states that:

- we operate throughout Australia and overseas and that as a result, the customer agrees that some of the uses and disclosures of their personal information may occur overseas; and
- the customer agrees that we may make such disclosures even if the disclosure is to an organisation overseas which is not subject to the privacy obligations which are equivalent to those which apply to us.

APP9 –Adoption, use or disclosure of government related identifiers

An identifier is a number, letter or symbol (or combination) assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. An individual's name is not an identifier.

Mega ICBC is prohibited from adopting as its own identifier of an individual a government related identifier, such as Tax File Numbers (TFNS), Medicare and pension numbers, unless the adoption is required under the law.

Further, Mega ICBC cannot use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for us to verify the identity of the individual for the purposes of our activities or functions.

There are further exceptions which include where the use or disclosure is required or authorised by a court/tribunal order; or is reasonably necessary to fulfil our obligations to an agency or State/Territory authority or for an enforcement related activity.

Mega ICBC monitors compliance with this obligation on at least a quarterly basis and reports any findings to the Risk and Compliance Committee (RCC).

APP10 –Quality of personal information

Mega ICBC must take reasonable steps to make sure that the personal information we collect is accurate, up-to-date and complete. If we use or disclose the personal information we must additionally ensure that the personal information is relevant to the purpose of the disclosure.

APP11– Security of personal information

Mega ICBC must take reasonable steps to protect the personal information we hold from misuse, interference and loss and also from unauthorised access, modification or disclosure.

We must also destroy or de-identify the information if it is no longer needed (unless it is required under an Australian law, or a court/tribunal order to retain the information).

Mega ICBC monitors compliance with this obligation on at least a quarterly basis and reports any findings to the Risk and Compliance Committee (RCC).

APP12– Access to personal information

Mega ICBC must provide individuals with access to and a copy of their personal information on request and within a reasonable period. This includes information collected from third parties, information received unsolicited and subsequently kept in records held, and opinions recorded about an individual.

Mega ICBC may choose to charge for access to personal information. Those charges must not be excessive and must not apply to lodging a request for access.

Mega ICBC does not have to give an individual access in a number of circumstances, which include:

- giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals; or
- the information relates to existing or anticipated legal proceedings between Mega ICBC and the individual; or

- giving access would reveal our intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- giving access would be unlawful; or
- we have reason to suspect that unlawful activity, or misconduct of a serious nature that relates to our functions or activities has been, is being or may be engaged in; and giving access would be likely to prejudice the taking of appropriate action; or
- giving access would be likely to prejudice enforcement related activities; or
- giving access would reveal evaluative information generated within Mega ICBC in connection with a commercially sensitive decision making process.

If Mega ICBC refuses access on any of the above grounds, or refuses to give access in the manner requested, then we have to give the individual a written notice setting out the reasons for the refusal and how to complain about the refusal.

The Mega ICBC Privacy and Spam Statement (Appendix A) notifies customers of their right of access to their personal information.

APP13 – Correction of personal information

If Mega ICBC is satisfied that the personal information we hold for an individual is inaccurate, out-of-date, incomplete or irrelevant or misleading; or if the individual requests a correction, then we need to correct that personal information within a reasonable period of time. We cannot charge the individual for making the correction.

If we have disclosed the personal information to someone else, then we need to notify them of the correction if the individual requests.

If Mega ICBC refuses to correct the personal information as requested by the individual, then we have to give the individual a written notice setting out the reasons for the refusal and how to complain about the refusal.

The Mega ICBC Privacy and Spam Statement (Appendix A) notifies customers that we will correct their personal information.