

defencebank.com.au

# **DEFENCE BANK PRODUCTS AND SERVICES**

## **CONDITIONS OF USE**

**Effective 01 February 2018**

# Conditions of Use

This document contains Terms and Conditions for:

## Savings Accounts

- > Basic Access
- > Budget Savings
- > Cadet Saver
- > Cash Management
- > Christmas Savings
- > Everyday Access
- > Flexi Term
- > General Insurance Savings
- > Investment Savings
- > iSaver
- > Kids Club Savings
- > Max eSaver
- > National Access
- > Offset
- > Pension Saver
- > Reservist Saver
- > Salary Saver
- > Teen Saver

## Term Deposits

- > Term Deposit

## Transaction Products

### Electronic Banking

- > Online Banking
- > Mobile Banking
- > Telephone Banking
- > BPAY®\*
- > Visa Debit Card
- > rediCARD
- > Osko

### Other Payment Services

- > Direct Debits
- > Direct Credits
- > Auto Transfers
- > Member Cheques

\* BPAY® is a registered trademark of BPAY Pty Ltd  
ABN 69 079 137 518.

# Contents

|   |    |
|---|----|
| Introduction.....   | 7  |
| Definitions.....  | 7  |
| Application of this DPS.....                                | 11 |
| ePayments Code.....   | 11 |
| Financial Claims Scheme.....                                | 11 |
| Varying Terms and Conditions.....                           | 12 |
| Complaints and Disputes Resolution Process.....             | 12 |
| Privacy Notice.....   | 14 |
| > What information can be disclosed?.....                   | 14 |
| > How we use your information.....                          | 15 |
| > Who can give or obtain information?.....                  | 16 |
| > Important information about credit reporting bodies... .. | 17 |
| > Security and Privacy Policy.....                          | 18 |
| > Contact Us.....   | 18 |

## **Part 1. General Information..... 18**

### **Section 1 – Account Opening..... 18**

|                                   |    |
|-----------------------------------|----|
| > Account Opening Procedures..... | 18 |
| > Taxation Implications.....      | 19 |
| > Tax File Number.....            | 19 |
| > Joint Accounts.....             | 19 |

### **Section 2 – Account Operation..... 20**

|   |    |
|---|----|
| > Account Signatories.....                    | 20 |
| > Deposits and Withdrawals.....               | 21 |
| > Right of Set-Off.....                       | 22 |
| > Mistaken Internet Deposits.....             | 22 |
| > Overdrawn Accounts.....                     | 22 |
| > Change of Personal and Account Details..... | 22 |
| > Closure of Accounts.....                    | 22 |
| > Dormant Accounts.....                       | 23 |
| > Statements.....                             | 23 |

## **Part 2. Savings Accounts Specific Information.... 24**

|                                       |    |
|---------------------------------------|----|
| > Savings Account Product Matrix..... | 24 |
| > Interest.....                       | 25 |
| > Fees and Charges.....               | 25 |
| > Government Charges.....             | 25 |

## **Part 3. Term Deposits Specific Information ..... 26**

|  |    |
|--|----|
| > Minimum Requirements.....                  | 26 |
| > Early Redemption of Your Term Deposit..... | 26 |
| > Term Deposits of 2 Years and Less.....     | 26 |
| > Term Deposits Over 2 Years.....            | 27 |
| > Term Deposit Confirmation.....             | 27 |
| > Grace Period.....                          | 27 |

|   |    |
|---|----|
| > Reinvestment .....                            | 27 |
| > Interest.....                                 | 27 |
| > Early Redemption Pre-payment Adjustment ..... | 28 |
| > Fees and Charges .....                        | 28 |
| > Government Charges .....                      | 28 |

**Part 4. Payment Facilities and Services..... 28**

**Section 1 – Electronic Banking ..... 28**

|   |    |
|---|----|
| > Electronic Banking Transaction Products Matrix.....   | 29 |
| > Benefits, Risks and Costs .....   | 30 |
| > Online Banking.....   | 30 |
| > Mobile Banking .....  | 31 |
| > Telephone Banking .....   | 32 |
| > BPAY (excluding Osko) .....   | 33 |
| > Visa Debit Card .....   | 34 |
| > rediCARD .....  | 35 |
| > ePayments Code .....  | 35 |
| > Protection of Your Passwords<br>and Personal Identification Number (PIN) .....              | 35 |
| > Fees and Charges .....  | 36 |
| > Merchant Surcharge .....  | 36 |
| > Government Charges .....  | 36 |
| > Specific Terms and Conditions – Electronic Banking ...                                      | 36 |
| > Introduction .....  | 36 |
| > IMPORTANT .....   | 37 |
| 1. Security and Access.....   | 38 |
| 2. VIP Access.....  | 39 |
| 3. Security Breaches .....  | 40 |
| 4. Using Electronic Banking (including BPAY) .....  | 41 |
| 5. Processing of Electronic Banking Transactions<br>(including BPAY) .....                    | 42 |
| 6. Future-dated BPAY Payments (excluding Osko) .....  | 43 |
| 7. Transaction Limits.....  | 44 |
| 8. Refusing Transaction Directions .....  | 44 |
| 9. Your Liability for Electronic Banking<br>Payments and Transfers.....                       | 44 |
| 10. Our Liability in Respect of Online Banking,<br>Mobile Banking and Telephone Banking ..... | 47 |
| 11. Resolving Errors on Account Statements.....   | 48 |
| 12. Transaction Recording .....   | 49 |
| 13. Transaction and Other Fees .....  | 49 |
| 14. Changes to Terms and Conditions.....  | 49 |
| 15. Cancellation of Electronic Banking Access .....   | 50 |

**Section 1A - Osko Payments ..... 51**

|   |    |
|---|----|
| 1. General.....                         | 51 |
| 2. Applicable Terms and Conditions..... | 51 |

|  |    |
|--|----|
| 3. Osko Services .....                   | 52 |
| 4. How to Use Osko .....                 | 52 |
| 5. How Osko Payments Work .....          | 52 |
| 6. Transaction Limits.....               | 53 |
| 7. Fees and Charges.....                 | 53 |
| 8. Notifications.....                    | 53 |
| 9. Liability .....                       | 53 |
| 10. Suspension and Termination.....      | 54 |
| 11. Privacy and Confidentiality .....    | 54 |
| 12. Changes to Terms and Conditions..... | 54 |
| 13. Definitions .....                    | 55 |

**Section 2 – Mistaken Internet Payments..... 55**

**Section 3 – Other Payment Facilities and Services ..... 60**

|                                    |    |
|------------------------------------|----|
| > Payment Services Matrix.....     | 60 |
| Fees and Charges.....              | 60 |
| Government Charges.....            | 61 |
| Specific Terms and Conditions..... | 61 |
| 1. Direct Debits .....             | 61 |
| 2. Direct Credits .....            | 62 |
| 3. Auto Transfers.....             | 63 |
| 4. Member Chequing.....            | 63 |

**Part 5. Visa Debit Card/rediCARD Conditions of Use..... 67**

|   |    |
|---|----|
| IMPORTANT .....   | 67 |
| Guidelines for Ensuring the Security of your Visa Debit Card/rediCARD and PIN ..... | 68 |
| 1. Introduction .....   | 69 |
| 2. Definitions .....  | 69 |
| 3. Application of these Terms .....   | 70 |
| 4. Code of Conduct .....  | 70 |
| 6. Protecting the PIN .....   | 71 |
| 7. Using the Visa Debit Card/rediCARD .....   | 71 |
| 8. Using the Visa Debit Card Outside Australia .....                                | 72 |
| 9. Withdrawal and Transaction Limits.....   | 73 |
| 10. Authorisations.....   | 74 |
| 11. Account Statements.....   | 74 |
| 12. Transaction Slips and Receipts .....  | 74 |
| 13. Subsidiary Cards.....   | 74 |
| 14. Renewal of the Visa Debit Card/rediCARD.....                                    | 75 |
| 15. Cancellation and Return of the Visa Debit Card/rediCARD .....                   | 76 |
| 16. Use After Cancellation or Expiry of the Visa Debit Card/rediCARD .....          | 77 |

|   |    |
|---|----|
| 17. Your Liability in Case the Visa Debit Card or rediCARD is Lost or Stolen or in Case of Unauthorised Use ..... | 77 |
| 18. How to Report Loss, Theft or Unauthorised Use of the Visa Debit Card/rediCARD or PIN .....                    | 80 |
| 19. Steps You Must Take to Resolve Errors or Disputed EFT Transactions .....                                      | 81 |
| 20. Transaction and Other Fees .....  | 83 |
| 21. Exclusions of Warranties and Representations.....   | 83 |
| 22. Malfunction .....   | 84 |
| 23. Changes to Conditions of Use.....   | 84 |
| 24. Miscellaneous .....   | 85 |

## **Part 6. Verified by Visa Terms ..... 85**

|  |    |
|--|----|
| IMPORTANT .....  | 85 |
| 1. Accepting these Terms .....   | 85 |
| 2. Definitions .....   | 86 |
| 3. Application of these Terms .....                                      | 86 |
| 4. Guidelines for Maintaining the Security of Your Visa Debit Card ..... | 86 |
| 5. Using the Verified by Visa Service .....                              | 86 |
| 6. Subsidiary Cardholders.....   | 87 |
| 7. Termination of Verified by Visa .....                                 | 87 |
| 8. Participating Online Merchants.....                                   | 87 |
| 9. Exclusion of Liabilities.....   | 88 |
| 10. Your Conduct .....   | 88 |
| 11. Your Liability .....   | 89 |
| 12. Errors .....   | 90 |
| 13. Changes to Terms .....   | 90 |

## **Part 7. PayID Terms ..... 90**

|  |    |
|--|----|
| 1. General.....  | 90 |
| 2. Applicable Terms and Conditions.....                  | 90 |
| 3. Creating a PayID .....                                | 91 |
| 4. Duplicated PayID .....                                | 92 |
| 5. PayID Name .....                                      | 92 |
| 6. Making Payments to a PayID .....                      | 92 |
| 7. Payments to Your PayID.....                           | 93 |
| 8. Maintaining PayID Details.....                        | 93 |
| 9. Locking Your PayID .....                              | 93 |
| 10. Transferring Your PayID to a Different Account ..... | 93 |
| 11. Closing Your PayID .....                             | 94 |
| 12. Liability .....                                      | 94 |
| 13. Privacy and Disclosure .....                         | 94 |
| 14. Definitions .....                                    | 95 |

# Introduction

Defence Bank's Products and Services Conditions of Use (DPS) contains important information about Defence Bank savings accounts, term deposits and the various payment facilities we offer. The DPS has been prepared to assist you in understanding the range of products we offer to our members. The information contained in this DPS will assist you to make an informed decision on whether to use any of the products covered by this DPS.

## Definitions

In this DPS:

**account** – a bank account you hold with us either in your own name solely or in your name and in the name of another.

**ADI** – Authorised Deposit-taking Institution.

**Auto Transfer** – Auto Transfers are payments you direct us to make periodically on your behalf and can be made to:

- > Accounts in your name with Defence Bank or other financial institutions, or
- > Accounts in the name of individuals, businesses, charities and the like with Defence Bank or other financial institutions.

**available balance** – the amount of any funds credited to your account but excluding:

- > Deposits received but not cleared
- > Interest accrued but not credited
- > Deposits in transit
- > Cheques written but not presented
- > Visa transactions not yet debited
- > Uncollected P2P payments.

**BECS** – the Bulk Electronic Clearing System.

**biller** – any person to whom you request we make a payment, other than us and in relation to BPAY payments means a biller who participates in BPAY.

**BPAY** – the electronic payment scheme called BPAY operated in co-operation between Australian financial institutions, which enables you to effect bill payments to billers who participate in BPAY, either via telephone or internet access or any other access method as approved by us from time to time.

**BPAY payment** – a payment transacted as part of the BPAY Scheme but does not include an *Osko payment*.

**Business Banking** – provides members operating a business account with the ability to transact via Electronic Banking.

**business day** – a day that is not a Saturday, a Sunday, a public holiday or a bank holiday.

**card** – the Visa Debit Card/rediCARD we have issued to you or to any other person at your request to enable you or that other person to access funds in your account(s) or any other card as we advise you from time to time.

**cardholder lost and stolen hotline** – a dedicated telephone service line established by the industry solely for cancelling rediCARDS and Visa Cards.

**cut off time** – the time that your BPAY payment or electronic transfer instruction must be received by us in order for those instructions to be processed that day.

**direct debit request** – the request between you and a biller authorising the biller to have funds debited from your account with Defence Bank.

**Electronic Banking** – facilities developed by Defence Bank to enable you, via telephone, online or mobile devices to make payments and transfers from your account and/or to obtain information and make requests about your account or generally about the products and services we offer. The expression Electronic Banking incorporates BPAY.

**ePayments Code** – the electronic payments Code issued by the Australian Securities and Investments Commission (ASIC).

**equipment requirements** – any equipment/software as specified by us that you will require to access and use Electronic Banking.

**facility** – an arrangement through which a person can perform transactions.

**Fees and Charges Schedule** – a document produced by us setting out fees and charges applicable to products and services provided by us.

**identifier** – information that you:

- > Know but are not required to keep secret, and
- > Must provide to perform a transaction.

Examples include an account number, serial number, a BSB number or the name of a payee.



**mistaken internet payment** – a payment through a “pay anyone” internet banking facility and processed by us through BECS where funds are paid into the account of an unintended recipient because you enter or select a PayID or a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:

- > Your error, or
- > You being advised of the wrong BSB number and/or identifier

but, does not include payments made using BPAY.

**mobile device** – a portable or handheld device such as a smartphone or tablet computer.

**NPP** – means the New Payments Platform, an open access infrastructure facilitating the making of fast payments in Australia.

**Mobile Banking** – where you access Online Banking via the Defence Bank App for mobile devices.

**Online Banking** – where you access Online Banking via the internet.

**Offset account** – any account where the balance is offset 100% against the balance of a linked mortgage loan.

**Osko** – the payment service provided by BPAY utilising the functionality of the NPP.

**Osko terms** – the terms that apply when Osko Payments are made or received as set out in Part 4, Section 1A of this DPS (Payment Facilities and Services – *Osko payments*).

**password** – a unique alphabetical and/or numeric combination and includes VIP Access and an SMS code where applicable. This will enable you to have secure access to Electronic Banking. A secure password is initially issued by us, but is then changed by you on first time use.

**payment** – a debit to your account of an amount and payment of that amount to a third party and includes BPAY.

**P2P payment** – means a payment we make pursuant to a request made by you that we pay to mobile or pay to email.

**receiving ADI** – an ADI which subscribes to the ePayments Code and whose customer has received an internet payment.

**SMS** – the telecommunications ‘short message service’ technology which may allow text messages to be sent to your mobile phone.

**telephone banking** – where you access Telephone Banking via the telephone.

**transaction authentication password** – a unique combination of alphabetical and numeric characters which gives you secure transactional processing and data update capability within Online Banking.

**transaction** – a payment or transfer to or from your account(s).

**transfer** – this is where your account is debited and your or another Defence Bank member's account is credited.

**unintended recipient** – the recipient of funds as a result of a mistaken internet payment.

**user ID** – the numerical or alphabetical identification, currently your member number, issued to you by Defence Bank which you use to access Electronic Banking in conjunction with your passwords.

**VIP Access** – A level two security feature you may register to use as provided by Symantec™ Validation & ID Protection (VIP) Access for Mobile which, when the App is downloaded to your mobile device, will provide you with an additional level of security when using Online Banking.

**you, your** or **member** – the Defence Bank member utilising a product or payment facility referred to in this DPS or any person authorised to act on behalf of the Defence Bank member.

In addition, references to:

- > **We, us,** or **Defence Bank** are references to Defence Bank Limited
- > **You** or **your** are references to you, the account holder(s) in respect of the account. See conditions for Joint Accounts in Part 1 of Section 1 which deem acts, omissions and failures to observe these conditions by certain other persons to be your acts, omissions and failures.

## **IMPORTANT**

You should read this DPS carefully. Always retain a copy for future reference.

## **Application of this DPS**

This DPS will apply immediately when you acquire one of the products or use any payment facility or service referred to in this DPS.

If the law implies any Terms and Conditions in relation to the products or facilities or services covered by this DPS which cannot be excluded, our liability under those implied Terms and Conditions will be limited to the maximum extent permitted by law.

In the event of any inconsistency between this DPS and any other Terms and Conditions applying to the products, the facilities or the services covered by this DPS, including those implied by law, then to the extent permitted by law the provisions of this DPS shall prevail.

## **ePayments Code**

We subscribe to the ePayments Code.

The ePayments Code regulates electronic payments including ATM, EFTPOS and credit card transactions, online payments, online and mobile banking and BPAY. It also provides key consumer protections in cases of fraud and unauthorised transactions and plays an important role in the regulation of electronic payment facilities in Australia.

## **Financial Claims Scheme**

When you acquire any of our deposit products described in this DPS you will be covered by the Financial Claims Scheme.

The Financial Claims Scheme (FCS) was established to protect depositors of Authorised Deposit-taking Institutions (banks, building societies and credit unions) from potential loss in the event that an institution fails or becomes insolvent.

The Scheme provides protection to depositors up to \$250,000 per account holder per Authorised Deposit-taking Institution, as well as seeks to provide access to these deposits in a timely manner.

The Scheme is administered by the Australian Prudential Regulatory Authority (APRA). Further information in relation to the Scheme can be obtained from the Financial Claims Scheme website ([fcs.gov.au](http://fcs.gov.au)).

## Varying Terms and Conditions

We are obliged to notify you of changes to this DPS in the following manner with respect to:

| Variation  | Period of Notice  |
|--|---|
| Introduction of a new fee or charge or increase in an existing fee or charge   | 30 days advance notice  |
| Change to method by which interest is calculated or the frequency with which it is debited or credited adverse to the account holder | 30 days advance notice  |
| Increase in liability for losses for electronic banking transactions   | 30 days advance notice  |
| Change in interest rate  | By date of change   |
| Change in penalty interest rate  | By date of change   |
| Other Changes  | Before the change or event occurs or as soon as practicable after, but not more than 3 months after, the change or event occurs |

We will notify you of changes in writing, by posting notice to our website or where authorised, electronically.

## Complaints and Disputes Resolution Process

Defence Bank is committed to providing Members with the best possible service. If at any time you feel we have not met our obligations – or you have a complaint about any of our products or services – please inform us so we can work towards a resolution. We will endeavour to deal with your complaint promptly, thoroughly and fairly.

If you have a complaint, we request you follow these steps:

In the first instance:

- > by visiting your local branch; or,
- > calling our Contact Centre on 1800 033 139; or,
- > emailing [info@defencebank.com.au](mailto:info@defencebank.com.au)

If a staff member cannot resolve the complaint/dispute to your satisfaction within 5 days, we will acknowledge receipt of the complaint to you in writing and we will also advise the procedures we will follow in investigating and handling your complaint.

During the time that a complaint/dispute is under further investigation we may also contact you to request further information to assist us in completing our review.

Within 21 business days of receiving a complaint, we will write to you advising the outcome of the investigation and the reason/s for our decision, or we may alternatively inform you that more time is required to complete the investigation. However, we will endeavour to respond to your complaint within a maximum of 45 business days from the date you lodged the complaint with us.

Defence Bank has also appointed a Customer Advocate whose role is to review complaints raised by members, where the member is not satisfied with the resolution arising from Defence Bank's internal dispute resolution process. The Customer Advocate operates independently and separately from Defence Bank's businesses and reports directly to the Chief Executive Officer (CEO).

As a member of Defence Bank you can elect to have your complaint referred to the Customer Advocate if you are not satisfied with the outcome of Defence Bank's dispute resolution processes for a further review and determination.

You may contact Defence Bank's Customer Advocate by calling (03) 8624 5448, or emailing [customeradvocate@defencebank.com.au](mailto:customeradvocate@defencebank.com.au) or writing to:

The Customer Advocate  
Defence Bank  
PO Box 14537  
Melbourne VIC 8001

If you do not think we have resolved your complaint to your satisfaction, you are also entitled to further pursue the matter – free of charge – to our External Dispute Resolution Scheme (provided it is within the scheme's terms of reference) whose details are provided below. You may also refer the matter to the relevant External Dispute Resolution Scheme at any time, but if our internal dispute resolution process is still in progress, they may request that our internal review be completed before considering the matter further.

Defence Bank's External Dispute Resolution Scheme provider's details are as follows:

Credit and Investments Ombudsman

Reply Paid 252

Sydney South NSW 1234

Phone 1800 138 422

Fax (02) 9273 8440

Email [info@cio.org.au](mailto:info@cio.org.au)

Web [cio.org.au](http://cio.org.au)

## Privacy Notice

This Privacy Notice outlines personal information we may collect from you and how we deal with that information in relation to the products and services referred to in the DPS and our rights and obligations in relation to that information. This Privacy Notice also outlines how we deal with your credit-related personal information which is relevant in circumstances where you apply for a loan or obtain credit from us.

### What information can be disclosed?

The *Privacy Act 1988* (Cth) allows us and other applicable persons to disclose personal information about you when related to the primary purpose for which it was collected. When providing credit to you, this personal information may include credit information such as:

- > details to identify you and verify your identity, such as your name, sex, date of birth, current and 2 previous addresses, your current and last known employer, and your driver licence number,
- > the fact that you have applied for credit and the amount or that we are a current credit provider to you, or that you have agreed to be a guarantor,
- > advice that payments previously notified as unpaid are no longer overdue,
- > information about your current or terminated consumer credit accounts and your repayment history,
- > payments overdue for at least 60 days and for which collection action has started,
- > in specified circumstances, that in our opinion you have committed a serious credit infringement,
- > the fact that credit provided to you by us has been paid or otherwise discharged, and

- > other information about credit standing, worthiness, history or capacity that credit providers can disclose under the Privacy Act, including a credit report.

We may also disclose personal information collected from you that is sensitive. This includes information about your health and wellbeing. Your sensitive information will only be disclosed where relevant to the purposes for which it was collected.

## **How we use your information**

When you apply for a membership, loan, deposit account or other products and services, we will collect personal information about you. We will use this information for the purpose of the relevant application and to assist us in providing you with the product or service applied for and for managing our business. We may also be required to collect, use and disclose information provided by you to comply with relevant laws and regulations.

When providing credit to you, our use of your personal information may include to:

- > assess your application for consumer or commercial credit or to be a guarantor for the applicant, assess your credit worthiness, manage your loan or the arrangements under which your loan is funded or collect overdue payments,
- > allow a credit reporting body to create and/or maintain a credit information file about you, and
- > if you are in default under a credit agreement, notify and exchange information with a credit reporting body, with other credit providers and any collection agent of ours.

If you are unable to provide us with the personal information requested, then we may be unable:

- > to provide you with the product or service you applied for,
- > to manage or administer your product or service,
- > to verify your identify or protect you from fraud, or
- > to tell you about other products or services that may be of interest or benefit to you.

We may also use personal information collected from you in order to tell you about other products and services. You can let us know at any time if you wish to no longer receive direct marketing materials from us.

## Who can give or obtain information?

For the purpose of providing products and services to you and managing our business, we may give information to or obtain information from:

- > external service providers we use such as:
  - (i) organisations we use to verify your identity,
  - (ii) payment systems operators including provision of cards, cheque books and cash,
  - (iii) mailing houses,
  - (iv) research consultants,
  - (v) medical professionals, where we seek to confirm your health status,
  - (vi) valuers, insurers (including mortgage insurers), re-insurers, claim assessors and investigators,
  - (vii) other financial institutions, or
  - (viii) organisations who maintain our computer systems and records and administer our products and services,
- > superannuation funds, where superannuation services are provided to you,
- > mercantile agencies and debt collecting agencies, if you have not repaid a loan as required,
- > our professional advisors, such as accountants, lawyers auditors and rating agencies,
- > real estate agencies,
- > commonwealth, state or territory authorities that give assistance to facilitate the provision of home loans to individuals,
- > other credit providers and their professional advisors,
- > your representatives, for example, lawyer, mortgage broker, financial advisor, conveyancer or attorney, as authorised by you, or
- > government and regulatory authorities, if required or authorised by law.

In addition, in connection with providing credit to you, we and the persons who are described as "Credit Providers" below may:

- > obtain a consumer and/or commercial credit report containing information about you from a credit reporting body,



- > obtain personal information about you from your employers and any references you may provide,
- > exchange credit information about you with each other, and
- > exchange credit information about you with any credit reporting body and any other provider of credit to you named in your credit application or a credit report from a credit reporting body.

The expression **Credit Providers** includes:

- > us
- > our related companies
- > other entities that may be involved in a securitisation arrangement which we use to fund your loan in the securitisation of your loan and any loan originator.

## **Important information about credit reporting bodies**

If you apply for any kind of credit, we may disclose information to a credit reporting body. That includes disclosing that you are in default under a credit arrangement or have committed a serious credit infringement if that is the case. (Specifically, we may disclose information to or collect information from Equifax Ltd, whose privacy policy is at [equifax.com.au](http://equifax.com.au), Dun & Bradstreet, whose privacy policy is at [dnb.com.au](http://dnb.com.au) and Experian, whose privacy policy is at [experian.com.au](http://experian.com.au))

Credit reporting bodies collect credit information about individuals which they provide as credit reports to credit providers and others in the credit industry to assist them in managing credit risk, collecting debts and other activities.

“Credit pre-screening” is a service for credit providers wishing to send direct marketing material about credit services. A credit reporting body uses information it holds to screen out individuals who do not meet criteria set by the credit provider. From 12 March 2014 credit reporting bodies must maintain a confidential list of individuals who have opted out of their information being used in pre-screening. To opt-out of credit pre-screening, contact the credit reporting body, using the contact details on their websites, referred to above.

You can also ask a credit reporting body not to use or disclose your personal information for a period if you believe on reasonable grounds that you have been or are likely to be a victim of fraud, including identity fraud.

## **Overseas disclosures**

On occasion, we do employ the services of overseas based organisations (the countries in which they are located are disclosed in our Privacy Policy published on our website at [defencebank.com.au](http://defencebank.com.au)). Where information is disclosed outside Australia, we will only do so on the basis that the information will be used for the purposes set out in this document.

## **Security and Privacy Policy**

### **Security**

We take reasonable steps to ensure that your personal information gathered by us (through our website or otherwise), and held by us is protected from misuse, interference and loss and from unauthorised access, disclosure or modification.

### **Privacy Policy**

Our Privacy Policy ([defencebank.com.au/privacy](http://defencebank.com.au/privacy)) provides additional information about how we handle your personal information. It sets out how you can ask for access to personal information we hold about you and if you deem necessary, how you can seek to correct that information. It also explains how you can complain about a breach of the Privacy Act or the Credit Reporting Code of Conduct, and how we will deal with your complaint. We will give you a copy of our Privacy Policy on request.

## **Contact Us**

### **Privacy Officer**

Our Privacy Officer's contact details are:

**Address:**

PO BOX 14537

Melbourne VIC 8001

**Telephone:** 1800 033 139

**Email:** [info@defencebank.com.au](mailto:info@defencebank.com.au)

(marked to the attention of the Privacy Officer)

## **Part 1. General Information**

### **Section 1 – Account Opening**

#### **Account Opening Procedures**

In accordance with the *Anti-Money Laundering/Counter-Terrorism Financing Act 2006* (Cth), we are required to

verify the identity of all our members before we can offer our products and services.

This usually involves collecting information about you, such as your name, address and date of birth and verifying that information against certain documents that you provide to us. These documents may include your current driver licence or passport etc.

Defence Bank reserves the right to provide a savings account to you and set the interest rate, maximum deposit and minimum deposit amounts.

## **Taxation Implications**

### **Income Tax**

Under the *Income Tax Assessment Act 1997* (Cth), tax may be payable on any interest earned on monies deposited in your account.

### **Tax File Number**

You are not obliged to disclose your tax file number to us. However, if you do not then we are obliged by law to deduct tax from any interest that you earn at the highest marginal rate plus the Medicare levy.

If you are a non-resident of Australia you are not required to provide a tax file number, however you will be subject to withholding tax on interest earned.

### **Joint Accounts**

Accounts may be conducted jointly with another person in the names of the individuals.

The following conditions apply:

- > Deposits may be accepted which are payable to either one or both of the account holders.
- > Liability for debts or overdrawn amounts is both joint and individual. For example, you will be jointly and individually liable should the account become overdrawn as the result of the actions of the other account holder, ie. them raising a direct debit which is paid in the absence of sufficient funds and the account becoming overdrawn.
- > Upon account opening you will be required to complete in writing an account signing authority which will specify who can operate the account. For example an account in joint names can be operated on an any one account holder to sign or both account holders to sign basis.

- > If one of the parties should die then any remaining balance shall be paid to the other account holder.
- > Any changes to who can operate the account will need to be in writing and signed by both account holders.
- > If Defence Bank is notified in writing of a dispute between account holders, we may require all account holders to sign to operate the account.
- > Defence Bank can send statements of account, changes to the DPS and other notices by mailing or emailing them to the first named account holder at the mailing address or email address we hold.
- > In the case of joint accounts, full access to the facilities of Electronic Banking is only available to members whose account operating authority is 'Either to Sign' or who have registered for Business Banking or Two to Sign Banking. Where the account operating authority is 'Either to Sign' then you are liable for any acts or omissions or failure to observe these conditions by the other account holders and any act or omission of another account holder or failure by another account holder to observe these conditions will be deemed to be your act, omission or failure as the case may be.
- > Members with joint accounts, multiple account holders and business accounts with account signing authorities requiring more than one signature and who have not registered for Business Banking, may be offered limited access to Electronic Banking. This limited access will permit the viewing of account detail and statements of account, however Online Banking will not be able to be used to conduct transactions.
- > These conditions apply to all accounts where the account signing authority requires two or more signatures. For the avoidance of doubt this includes personal accounts, business accounts, Mess accounts and the like.

## **Section 2 – Account Operation**

### **Account Signatories**

At the time of opening the account, we will provide you with a form on which you will be required to authorise in writing who will have authority to operate your account.

## **Deposits and Withdrawals**

### **Deposits**

Deposits to accounts may be made:

- > In person at a branch
- > In person at a National Australia Bank (NAB) branch. NAB may charge a fee for this service. You will need to supply BSB 833-205 together with a link number, which will direct the deposit to your specific Defence Bank account. The link number is available by calling 1800 033 139 or from your Defence Bank branch.
- > In person at Bank@Post outlets (a Visa or rediCARD is required)
- > By Direct Credit or Internal Transfer
- > By Inward Electronic Transfer
- > By Osko Payment
- > By Mail (cash should not be forwarded by mail).

### **Withdrawals**

Withdrawals from accounts may be made:

- > In person at a branch
- > In person at Bank@Post outlets (Visa or rediCARD required)
- > By personal cheque
- > By Defence Bank Cheque
- > By Visa transaction
- > By Automatic Teller Machine (ATM) and Point of Sale (POS) terminal (Visa or rediCARD required)
- > By telegraphic transfer (the method for a payment to be made to an international bank account)
- > By authorised Direct Debit
- > By authorised Auto Transfer
- > By Online Banking
- > By Osko Payment
- > By Mobile Banking
- > By Telephone Banking
- > By BPAY

## **Right of Set-Off**

If you have more than one account (including a loan account) with us, we may set off the credit balance of any of your deposit accounts against any debt owing by you to us from time to time. This means that we can transfer money from one account to another if one or more deposit accounts are overdrawn without prior authorisation, or a loan repayment has not been made. We will inform you if we exercise this right of set-off.

## **Mistaken Internet Deposits**

Where a deposit is made to your account via an internet banking facility, and the sender of those monies asserts that they made a mistaken internet payment, then we are obliged to investigate the matter and may be required to return those funds to the sender's ADI. In those circumstances we are regarded as a "receiving ADI" and the obligations imposed on us in that capacity are as set out in Section 2 of Part 4 of the DPS.

We may debit or place a stop on your account at any time in respect to a mistaken internet deposit until such time as we have complied with our obligations under the ePayments Code in our capacity as a receiving ADI.

## **Overdrawn Accounts**

You must not overdraw your account without our prior agreement. Any amount overdrawn without prior agreement is repayable immediately. We may at our discretion allow the overdrawing of an account and impose a fee each time we permit an account to be overdrawn, or for a debit balance to increase once it is already overdrawn.

## **Change of Personal and Account Details**

You should notify us promptly of any changes to your details, including change of name, address, telephone number or email address. We will not be responsible for any errors or losses associated with changes to your details where we have not received prior notice.

## **Closure of Accounts**

Requests to close accounts must be signed in accordance with the account signing authority. All unused cheques and Visa or rediCARDS must be surrendered for cancellation prior to closure. Direct debits and direct credits attached to the particular account must be cancelled or amended and this is the responsibility of the account holder to arrange.

Similarly, requests from one joint account holder where the account signing authority is 'either to sign' to change to 'all to sign' can only be accommodated where all unused cheques and Visa or rediCARDS are surrendered.

We may close an account of yours at any time without cause. If we do so, we will give you at least 14 days advance notice. Where your account is in credit we will pay you the amount of the credit balance.

## **Dormant Accounts**

If you have not initiated a transaction on your savings accounts for a period of more than 12 months, the accounts will be classified as dormant and an annual maintenance fee may apply. For details refer to the Fees and Charges Schedule. No interest will be paid on dormant accounts. Accounts declared dormant may result in your membership with Defence Bank being terminated. You may apply to have your membership reinstated.

## **Statements**

Account statements are issued on the following basis:

| <b>Statement Name</b> | <b>Statement Cycle</b>  |
|-----------------------|---|
| Overdraft             | Issued monthly  |
| All savings accounts  | Issued quarterly at the end of months March, June, September and December |

Statements may be issued on a monthly basis by request (a charge applies for this service).

We will post account statements to your mailing address as held in our records, or where authorised, electronically.

eStatements are available via Defence Bank Online Banking.

To receive eStatements you need to register via Defence Bank Online Banking. Once registered you will no longer receive your statement via the post and will also be able to view any previous statement outside of the current statement period (classified as a previous statement).

You can also request copies of previous statements.

Applicable fees and charges are detailed in the Fees and Charges Schedule.

If you notice any errors or unauthorised transactions detailed in your statement, please notify us without delay.

# Part 2. Savings Accounts Specific Information

## Savings Account Product Matrix

The following matrix sets out relevant features for each savings account product:

| Account Type                 | Visa/<br>rediCARD<br>ATM/<br>EFTPOS | Over<br>draft<br>Facility | Cheque<br>Book | BPAY | Bank @<br>Post | Direct<br>Entry | Bank<br>Chq | Min<br>Bal | Osko/<br>PayID | Electronic<br>Banking<br>Transfers |
|------------------------------|-------------------------------------|---------------------------|----------------|------|----------------|-----------------|-------------|------------|----------------|------------------------------------|
| Basic Access                 | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Budget Savings               | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Cadet Saver                  | ✓                                   | X                         | X              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Cash Management              | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Christmas Savings            | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Everyday Access              | ✓                                   | ✓                         | ✓              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Flexi Term                   | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| General Insurance<br>Savings | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Investment Savings           | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| iSaver                       | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Kids Club Savings*           | X                                   | X                         | X              | X    | X              | ✓               | ✓           | \$0        | X              | X                                  |
| Max eSaver                   | X                                   | X                         | X              | ✓    | X              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| National Access              | ✓                                   | ✓                         | ✓              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Offset+                      | ✓                                   | X                         | ✓              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Pension Saver#               | ✓                                   | X                         | ✓              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Reservist Saver              | ✓                                   | X                         | ✓              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Salary Saver                 | ✓                                   | ✓                         | ✓              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |
| Teen Saver                   | ✓                                   | X                         | X              | ✓    | ✓              | ✓               | ✓           | \$0        | ✓              | ✓                                  |

Please note: you may have to provide notice for large cash withdrawals. Please contact your local branch or call 1800 033 139 for details.

### Key to table

\* available to children under 12 years of age. Account to be held in child's name.

# pension to be allocated directly to account.

+ offset 100% against balance of linked mortgage loan.



## Interest

> Interest is calculated daily and is credited as follows:

| Account Type  | Interest Credited  |
|---|--|
| Basic Access, Budget Savings, Kids Club Savings, National Access, Salary Saver, Everyday Access, General Insurance Savings, Teen Saver, Cadet Saver and Reservist Saver | 31 March each year   |
| Cash Management   | Last day of each month   |
| Christmas Savings   | 31 October each year   |
| Flexi Term  | Last day of each month   |
| Investment Savings  | 31 March and 30 September each year  |
| iSaver  | Last day of each month   |
| Max eSaver  | Last day of each month – at least one deposit and no withdrawals are required to be conducted during the month to receive bonus interest |
| Offset  | Balance is offset 100% against linked mortgage loan  |
| Pension Saver   | Last day of February, May, August and November each year   |

> The Interest Rate Schedule which details rates offered for each savings account and for tiered rates where applicable is available at your nearest branch, by visiting [defencebank.com.au](http://defencebank.com.au) or by calling 1800 033 139.

## Fees and Charges

The fees and charges applicable to Defence Bank Savings Account Products are detailed in the Fees and Charges Schedule. Transaction fees may be charged (refer to the Fees and Charges Schedule which is available at your nearest branch, by visiting [defencebank.com.au](http://defencebank.com.au) or by calling 1800 033 139).

## Government Charges

We reserve the right to debit your savings account with any applicable government charges, including any government charges introduced after the account is established.

## **Part 3. Term Deposits Specific Information**

### **Minimum Requirements**

Term Deposits are fixed interest earning accounts, with agreed terms, or other terms subject to our agreement, details of which can be obtained from our Interest Rate Schedule. This is available at your nearest Defence Bank branch, by visiting [defencebank.com.au](http://defencebank.com.au) or by calling 1800 033 139.

The interest rate payable will be the interest rate specified on the Certificate of Investment applicable to your Term Deposit. Interest rates may vary dependent on the term and the amount of the deposit.

The interest rate specified is guaranteed provided you accept our conditions in relation to limits which may apply to the amount of the deposit at lodgement, that the deposit is held for the term specified in the Certificate of Investment and that no withdrawals or additional deposits are made during the agreed term.

We have the right to accept or refuse any deposit and to set the maximum or minimum amounts of a deposit and the term of the deposit.

### **Early Redemption of Your Term Deposit**

- > The Term Deposit is intended to be held for the agreed term, until maturity. Despite this, we may permit you to access your Term Deposit amount before maturity.
- > A pre-payment adjustment and a fee may apply. The extent of the pre-payment adjustment will depend on the percentage of the original term elapsed when early access is given.

Applicable fees and charges are detailed in the Fees and Charges Schedule.

### **Term Deposit of 2 Years and Less**

- > You may ask us to release your Term Deposit before maturity by calling us or visiting your local branch during business hours. You must give us at least 24 hours' notice. If we agree to release the Term Deposit we will tell you within one (1) business day of your request.

## **Term Deposits Over 2 Years**

- > Where the initial term of your Term Deposit is more than 2 years, you may access your Term Deposit amount before maturity. You will however need to provide us with 24 hours' notice. Please call us on 1800 033 139 or visit your nearest Defence Bank branch to discuss.

## **Term Deposit Confirmation**

We will provide you with written confirmation of your Term Deposit detailing the deposit amount, interest rate and length of the term shortly after we set up or renew your term deposit.

## **Grace Period**

We allow a five business day grace period after your Term Deposit matures during which you can change your renewal instructions.

## **Reinvestment**

Prior to the maturity of your Term Deposit you will receive a letter advising you of the approaching maturity. If you wish to redeem or vary the terms of the Term Deposit, your signed, written instructions are required prior to the expiration of the grace period. Your request will be actioned on the maturity date, the next business day, or within the grace period. If we do not receive instructions from you, your Term Deposit and interest will automatically be reinvested on the maturity date for the same term and at the then current published Term Deposit interest rate.

If the same term is no longer available then your Term Deposit will be reinvested at the closest standard term (ie non-premium certificate) to the original term. Any requests for variations to the terms of your Term Deposit received after the grace period has expired, may incur a pre-payment adjustment and a fee.

General Withholding Tax may be debited from your interest if a Tax File Number or ABN has not been provided.

## **Interest**

Interest is calculated on the daily balance. Interest is paid on the date of maturity. Where terms exceed 12 months, interest is capitalised annually, interest payable in respect of the last 12 months or part thereof is added to the balance at maturity or on the next business day. Any variation to this method of interest payment is considered a 'special condition' and must be agreed to by us prior to the deposit

maturing. The interest rate applicable to the different terms and amounts of investment are outlined in Defence Bank's Interest Rate Schedule. A copy of the Schedule is available at your nearest Defence Bank branch, by visiting [defencebank.com.au](http://defencebank.com.au) or by calling 1800 033 139.

### **Early Redemption Pre-payment Adjustment**

If you require your funds before the maturity date of the term, either partially or in full, a pre-payment adjustment and fee may apply.

| <b>Percentage of the term lapsed</b> | <b>Adjustment to be applied as a % of your interest rate</b> |
|--------------------------------------|--|
| 0% to less than 20%                  | 90%  |
| 20% to less than 40%                 | 80%  |
| 40% to less than 60%                 | 60%  |
| 60% to less than 80%                 | 40%  |
| 80% to less than 100%                | 20%  |

### **Fees and Charges**

The fees and charges applicable to Defence Bank Term Deposit products are detailed in the Fees and Charges Schedule.

### **Government Charges**

We reserve the right to debit your Term Deposit account with any applicable government charges as a result of using a Defence Bank Term Deposit account, including any government charges introduced after the account is established.

## **Part 4. Payment Facilities and Services**

These comprise:

- > Electronic banking payment facilities
- > Other payment facilities and services

### **Section 1 – Electronic Banking**

Defence Bank's Electronic Banking products comprise:

- > Online Banking
- > Mobile Banking

- > Telephone Banking
- > BPAY
- > Visa Debit Card
- > rediCARD

## Electronic Banking Transaction Products Matrix

The following matrix details the availability of Electronic Banking facilities for Defence Bank savings accounts.

| Account Type              | Online/<br>Mobile<br>Banking | Telephone<br>Banking | Visa<br>Debit/<br>rediCARD | Osko/<br>PayID | ATM/<br>POS | BPAY |
|---------------------------|------------------------------|----------------------|----------------------------|----------------|-------------|------|
| Basic Access              | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| Budget Savings            | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| Cadet Saver               | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Cash Management           | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| Christmas Savings         | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| Everyday Access           | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Flexi Term                | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| General Insurance Savings | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| Investment Savings        | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| iSaver                    | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| Kids Club Savings         | X                            | X                    | X                          | X              | X           | X    |
| Max eSaver                | ✓                            | ✓                    | X                          | ✓              | X           | ✓    |
| National Access           | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Offset                    | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Pension Saver             | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Reservist Saver           | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Salary Saver              | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |
| Teen Saver                | ✓                            | ✓                    | ✓                          | ✓              | ✓           | ✓    |

Approval for you to use an electronic banking service is solely at our discretion and we reserve the right to suspend or cancel access to an electronic banking service without prior notice to you.

## Benefits, Risks and Costs

The following is a summary of Electronic Banking products.

### Online Banking

#### Benefits

- > 24 hours a day, 7 days a week access to Defence Bank accounts via our website [defencebank.com.au](http://defencebank.com.au)
- > View account balances
- > View and print transaction listings
- > Transfer funds to any Defence Bank account
- > View interest details
- > View statements of account
- > View eStatements
- > Pay bills electronically via BPAY
- > Receive bills via BPAY View
- > Set up and manage one off or regular payments
- > Electronically transfer funds to another financial institution (credit card payments cannot be forwarded through this service)
- > Electronically transfer funds overseas
- > Apply for a loan
- > Redraw from your home or personal loan
- > Register for VIP Access
- > Register a PayID
- > Manage SMS alerts
- > Set up Mobile Banking
- > Personalise your own screen settings
- > Limited ability to recover mistaken internet payments made to unintended recipients except for BPAY
- > Activate your Defence Bank Visa Card or rediCARD
- > Secure passwords are issued upon registration
- > Online changes to account details and to remit funds electronically requires the use of a transaction authentication password
- > Access via compatible mobile phone, mobile device, PC or other access device
- > Open a savings account

## **Risks**

- > Need to ensure security of access to your account passwords
- > Need to ensure security of any access device such as a PC, mobile phone or mobile device
- > Account operation via internet may incur unauthorised loss of funds if appropriate security precautions are not undertaken, such as installation of anti-virus, anti-spyware, firewall software and changing your passwords on a regular basis
- > Risk of unauthorised access to your account if passwords can be easily identified
- > Account holder may be liable for unauthorised transactions arising from a failure to properly secure passwords against loss, theft or misuse
- > All precautions are taken in respect of online banking transactions, however the security of electronic transfer transactions can never be guaranteed, particularly in electronic media such as the internet

## **Costs**

- > Dependent on your account type, fees may apply for each electronic transfer and BPAY transaction to an external financial institution/biller
- > For details of these and any other fees refer to the Fees and Charges Schedule

## **Mobile Banking**

### **Benefits**

- > 24 hours a day, 7 days a week access to Defence Bank accounts via your mobile device
- > View account balances
- > View transaction listings
- > Transfer funds to any other Defence Bank account
- > Pay bills electronically via BPAY
- > View regular payments
- > Electronically transfer funds to another financial institution (credit card payments cannot be forwarded through this service)
- > Manage SMS alerts
- > Register a PayID

## **Risks**

- > Need to ensure security of access to your passwords
- > Need to ensure security of any mobile device
- > Risk of unauthorised access to your account if passwords can be easily identified
- > Account holder may be liable for unauthorised transactions arising from a failure to properly secure passwords against loss, theft or misuse
- > All precautions are taken in respect of mobile banking transactions, however the security of electronic transfer transactions can never be guaranteed, particularly in electronic media such as the internet

## **Costs**

- > Dependent on your account type, fees may apply for each electronic transfer and BPAY transaction to an external financial institution/biller
- > For details of these and any other fees refer to the Fees and Charges Schedule

## **Telephone Banking**

### **Benefits**

- > Secure 24 hour automated telephone banking system that can be accessed using a touch-tone phone
- > Check account balances
- > Check previous transactions
- > Transfer funds between Defence Bank accounts
- > Pay bills using BPAY
- > Check interest earned in the current and previous financial year
- > Activate your Defence Bank Visa Card or rediCARD
- > Order posted/faxed transaction listings
- > Change password
- > Request a loan application form be posted
- > Leave a message for Defence Bank
- > A secure password is issued on registration



## **Risks**

- > Need to ensure security of access to your account passwords
- > Risk of unauthorised access to your account if passwords can be easily identified
- > Account holder may be liable for unauthorised transactions arising from a failure to properly secure the passwords against loss, theft or misuse

## **Costs**

- > Dependent on account type, fees may be payable for BPAY transactions conducted via Telephone Banking
- > For details of these and any other fees refer to the Fees and Charges Schedule

## **BPAY (excluding Osko)**

### **Benefits**

BPAY is a network of Billers who allow you to pay your bills through Online, Mobile or Telephone Banking.

You can pay most of your bills using BPAY including telephone, electricity, gas or water bills. Just look for the BPAY logo and references on your bill.

To pay a bill using BPAY via Online, Mobile or Telephone Banking, the following details are required:

- > the Biller Code
- > the Customer Reference Number
- > the amount

An *Osko Payment* is not a BPAY Payment

### **Risks**

- > All precautions are taken in respect of BPAY transactions, however the security of electronic transfer transactions can never be guaranteed. In online mediums which require use of the internet, there is always a risk of interception of data by an unauthorised party or hacker.

### **Costs**

- > Dependent on your account type, a fee may be payable for each BPAY transaction
- > For details of these and any other fees refer to the Fees and Charges Schedule

## **Visa Debit Card**

### **Benefits**

- > A Visa Debit Card provides you with access to funds held in your Everyday Access, National Access, Cadet Saver, Teen Saver, Reservist Saver, Salary Saver, Offset or Pension Saver Account
- > Access may be gained through Automatic Teller Machines (ATMs), Bank@Post, online and merchant locations (POS)
- > Access via ATMs and participating merchants may be made within Australia and overseas
- > Increased access to your Defence Bank savings account
- > Transactions not limited to Defence Bank standard business hours

### **Risks**

- > You need to ensure the security of your Visa Debit Card
- > Need to ensure security of access to your account ie your PIN
- > Risk of unauthorised access to your account if your PIN can be easily identified
- > Some merchants and EFTPOS terminals may impose a surcharge for making a transaction. You should enquire as to whether any surcharge applies before confirming the transaction

### **Costs**

- > Dependent on your account type, a fee may be charged for excess EFTPOS transactions. If you use a non rediATM the owner of the ATM may charge you a fee for using their ATM. This fee will be displayed on the screen prior to the transaction being processed and you will have a choice to cancel the transaction before it proceeds
- > Dependent on your account type a monthly fee may apply for a Visa Debit Card/s
- > For details of these and any other fees refer to the Fees and Charges Schedule

## **rediCARD**

### **Benefits**

- > rediCARD provides you with access to funds held in your Everyday Access, National Access, Salary Saver, Reservist Saver, Teen Saver, Cadet Saver, Offset or Pension Saver Account within Australia only
- > rediCARD access to your account may be gained via ATMs and POS facilities throughout Australia
- > Increased access to funds in your Defence Bank savings account
- > Transactions not limited to Defence Bank standard business hours

### **Risks**

- > You need to ensure the security of your rediCARD
- > Need to ensure security of access to your account ie your PIN
- > Risk of unauthorised access to your account if your PIN can be easily identified

### **Costs**

- > Dependent on your account type, a fee may be charged for excess POS transactions. If you use a non rediATM the owner of the ATM may charge you a fee for using their ATM. This fee will be displayed on the screen prior to the transaction being processed and you will have a choice to cancel the transaction before it proceeds
- > For details of these and any other fees refer to the Fees and Charges Schedule

## **ePayments Code**

The relevant provisions of the ePayments Code apply when you use our electronic banking facilities to access and transact on your accounts.

## **Protection of Your Passwords and Personal Identification Number (PIN)**

- > You must keep your passwords and PIN secure at all times. Failure to do so may increase your liability for loss.

### **YOU MUST NOT:**

- > Use your birth date or an alphabetical code which is a recognisable part of your name as a password or select a numerical code which has four sequential numbers

- > Disclose your passwords or PIN to any person including family members and friends
- > Allow any other person to see you entering or overhear you providing your passwords or PIN
- > Record your passwords or PIN on your card or on any article carried with or placed near your card that is liable for loss, theft or abuse at the same time as your card

## **Fees and Charges**

Defence Bank fees and charges applicable to the Electronic Banking facilities are detailed in the Fees and Charges Schedule. The Fees and Charges Schedule and our brochure titled 'Tips for reducing your banking fees with Defence Bank' are available at your nearest Defence Bank branch, by visiting [defencebank.com.au](http://defencebank.com.au) or by calling 1800 033 139.

## **Merchant Surcharge**

Some merchants and EFT terminals charge a surcharge for making EFT transactions. You should ask whether any surcharge applies and the amount of any surcharge before confirming the transaction. Once you have confirmed a transaction you will not be able to dispute the surcharge.

## **Government Charges**

We reserve the right to debit your savings account with any applicable government charges as a result of using an electronic banking facility, including any government charges introduced after the account is established.

## **Specific Terms and Conditions – Electronic Banking**

These Terms and Conditions specifically cover our electronic banking products, namely Online Banking, Mobile Banking, Telephone Banking, Digital Wallet, BPAY and Visa Debit/rediCARD.

Additional Mobile Banking and Digital Wallet Terms and Conditions apply and are specified when you download the relevant App for that service.

## **Introduction**

You will need to be registered to use Online Banking, Mobile Banking or Telephone Banking. To register, call 1800 033 139, visit your nearest Defence Bank branch, or download the application forms from [defencebank.com.au](http://defencebank.com.au). After registering for Online Banking, you can download the Mobile Banking App from the App Store or the Google Play Store.

## IMPORTANT

These Terms and Conditions will govern your access to Electronic Banking. It is therefore important that you read these Terms and Conditions carefully before you use Electronic Banking. These Terms and Conditions must be read in conjunction with your Visa Card/rediCARD Conditions of Use, as well as the Terms and Conditions that apply to your use of the Mobile Banking App if you download and use the App.

These Terms and Conditions of use and accompanying information operate alongside any legal rights held by you or Defence Bank, but do not replace, although may limit, any of those rights.

We strongly recommend that you stay abreast of this guide as it contains information that could be important to you in the future.

We will issue you with an initial password to enable you to log into Online Banking. Once you log in, you will need to set your transaction authentication password immediately to protect yourself from fraud. This transaction authentication password will enable you to make transactions and update personal details. You may also register for VIP Access, which will replace your transaction authentication password and facilitate a greater daily transaction limit. Details of which are available on our website at [defencebank.com.au](http://defencebank.com.au).

To safeguard your usage of Electronic Banking, we recommend that you take these steps:

- > Change your initial system generated password when you first use Online Banking, Mobile Banking or Telephone Banking
- > Change your passwords at regular intervals (passwords issued by Defence Bank expire after 14 days)
- > Never reveal your passwords to anyone
- > Never write your passwords down
- > Utilise all of the security provisions that we make available
- > Immediately notify us of any change of address. Where doubt exists about the security of your passwords, you may change your passwords, by selecting the 'Change Password' option from the menu in either Online Banking (for your Online Banking password), Telephone Banking (for your Telephone Banking password), or Mobile Banking (for your Mobile Banking password).

In the case of a joint membership where the account operating authority is 'Either to sign', we will issue each member with individual passwords. The system will require each member to change these passwords subsequent to the first time these passwords are used.

Online Banking, Mobile Banking and Telephone Banking enable you to conduct value transactions, such as BPAY and funds transfer, to be processed from your accounts, which are accessed by use of your member number and passwords. Over time, new functionality may also be added.

Please ensure that you are happy for value transactions to be carried out using this service. If any new functionality involving value transactions causes you concern, please advise us without delay so that we can discuss alternatives which may better suit your needs.

Defence Bank can be contacted:

- > By telephone on (03) 8624 5888 or 1800 033 139 between 8am and 8pm, on business days (AEST)
- > By facsimile on (03) 8624 5892
- > By email via [info@defencebank.com.au](mailto:info@defencebank.com.au)
- > Via our website at [defencebank.com.au](http://defencebank.com.au)
- > By mail to our Registered Office:  
Defence Bank  
PO Box 14537  
Melbourne Vic 8001.

If you experience difficulties with any Electronic Banking, please telephone Defence Bank on (03) 8624 5888 or 1800 033 139, 8am to 8pm, on business days (AEST).

By accessing Electronic Banking you will be taken to have read, understood and accepted these Terms and Conditions. These Terms and Conditions apply to all Defence Bank Electronic Banking transactions and you will be legally bound by them.

## **1. Security and Access**

- 1.1. You must maintain at all times a valid email address for delivery of transaction confirmation for Online Banking. Transaction confirmation will be provided at the discretion of Defence Bank.
- 1.2. You agree to promptly notify us of any change of your email address.

- 1.3. It is your responsibility to select, obtain and maintain any equipment/software and communications facility which may be necessary to gain access to and to use Electronic Banking.
- 1.4. It is your responsibility to obtain, maintain and comply with the equipment requirements as advised and amended from time to time by us which may be necessary for you to access and use Electronic Banking.
- 1.5. It is your responsibility to utilise the security provisions provided by Defence Bank to ensure the security of your transactions.
- 1.6. You acknowledge that the Mobile Banking App will not enable you to utilise the same functionality as Online Banking.
- 1.7. You acknowledge that not all internet enabled mobile devices are capable of accessing and using Online Banking or the Mobile Banking App and mobile device access to Online Banking or Mobile Banking outside Australia will be dependent on the functionality of your telecommunications provider's international roaming services.
- 1.8. You acknowledge that in accessing Electronic Banking you may incur costs from your telecommunications provider and are responsible for those costs.

## **2. VIP Access**

- 2.1. You may register to use VIP Access by:
  - (i) Registering for Online Banking,
  - (ii) Accepting the VeriSign® Identity Protection End User Agreement, and
  - (iii) Downloading the VIP Access App to your mobile phone or mobile device.
- 2.2. You acknowledge that not all internet enabled mobile devices are capable of using VIP Access.
- 2.3. Any VIP Access security code issued to you is personal to you.
- 2.4. Use of VIP Access provides an additional level of security for your Online Banking and must not be shared with anyone else.
- 2.5. Your VIP Access security code is used to authenticate transactions made via Online Banking. Your VIP

Access security code is your electronic password and mechanism to authorise transactions and suitable care and responsibility must be taken regarding its use and access.

- 2.6. Your VIP Access App resides on your nominated mobile device and it is your responsibility to ensure that you take care of your mobile device and prevent unauthorised access in the same way as you are required to protect the security of your other passwords.
- 2.7. The types of accounts you can access will not change when you register for VIP Access. However, once registered you will need to use your VIP Access security code every time you use Online Banking to transact or update data, except for those transactions made via Mobile Banking.
- 2.8. You may cancel your VIP Access at any time by contacting us.
- 2.9. You must keep your VIP Access safe and secure and contact us immediately if your nominated mobile device is lost, stolen or misused. We will then deactivate your VIP Access.

### **3. Security Breaches**

- 3.1. In this condition, the expression 'you' includes any person to whom a card or password has been issued or given with your consent.
- 3.2. If you suspect for any reason that anyone has discovered or may have discovered your passwords, then you must change your passwords by selecting the 'Change Password' option from the menu in either Online Banking (for Online Banking password changes) or Mobile Banking (for Mobile Banking password changes) or Telephone Banking (for Telephone Banking password changes).
- 3.3. If you also suspect that your card or your card details are accessible to that person (particularly if you are unable for any reason to change your password) then we recommend you cancel your card by calling the

**Cardholder lost and stolen card hotline  
1800 648 027 Australia wide, 7 days a week,  
24 hours a day**



- 3.4. If your card is lost or stolen or you suspect for any reason that someone has a record of your card details and may use them to access your account, you must report this to the Cardholder lost and stolen card hotline to have your card cancelled.
- 3.5. The Cardholder lost and stolen card hotline will give you a reference number. Please retain this number as evidence of the date and time of your report.
- 3.6. If the Cardholder lost and stolen card hotline is not operating at the time notification is attempted, the loss, theft or unauthorised use must be reported to Defence Bank during business hours, or via email [info@defencebank.com.au](mailto:info@defencebank.com.au) or the Cardholder lost and stolen card hotline (when available) whichever is the sooner.

If the Cardholder lost and stolen card hotline is not operating at the time you attempt to call to cancel your card, we will be liable for any losses which:

- (i) Are incurred after you attempt to call and
- (ii) Are due to the failure to cancel.

BUT ONLY if the loss, theft or unauthorised use is reported to us or the hotline within a reasonable time of either becoming available.

- 3.7. The Cardholder lost and stolen card hotline is a dedicated call line established and operated by the industry solely for cancelling rediCARDS and Visa Cards. It cannot assist you with Defence Bank Electronic Banking Channels or BPAY enquiries, system problems or password issues. If you report your card as lost or stolen to the Cardholder lost and stolen card hotline, you should then also contact us on the next business day, to advise us of this cancellation, the reference number provided, and to arrange a replacement card.

#### **4. Using Electronic Banking (including BPAY)**

- 4.1. This section applies when you use Electronic Banking to make BPAY payments but does not apply to *Osko payments*.
- 4.2. You may make transactions of the type permitted by us and BPAY from time to time.
- 4.3. BPAY can be used to pay bills bearing the BPAY logo. We will advise you if and when other transactions can be made using BPAY.

- 4.4. We will debit the value of each payment or transfer and any applicable fees to the account from which the relevant payment or transfer is made.
- 4.5. If you instruct us to make any payment or transfer, but close the account to be debited before the payment or transfer is processed, you will remain liable for any dishonour fees incurred in respect of that transaction and we may exercise our rights of set-off under the condition in Section 2 of Part 1 – Account Operation, Right to Set-Off.
- 4.6. We will take all reasonable steps to ensure that the information we make available to you through Electronic Banking is correct and regularly updated.
- 4.7. We will not be liable for any loss you suffer due to the inaccuracy, error or omission of information in Electronic Banking, due to the failure of our system or communications network including ancillary equipment or in any other circumstance beyond our reasonable control.

## **5. Processing of Electronic Banking Transactions (including BPAY)**

- 5.1. This condition applies to the processing of all Electronic Banking transactions, including BPAY payments.
- 5.2. A payment or transfer using Electronic Banking is irrevocable, except for future-dated BPAY payments as specified in condition (6) in Part 4. You cannot stop a payment or transfer once you have instructed us to make it and we cannot reverse it.  
  
However, in the case of a mistaken internet payment to an unintended recipient we may be able to request a return of funds as long as the payment was not made using BPAY. See Section 2 of this Part for details.
- 5.3. A payment, other than a BPAY payment, is deemed as being received by the party to whom it is directed, generally on the next business day after you direct us to make it.
- 5.4. A transfer is deemed as made and received into the account specified generally on the same business day as you direct us to make it.
- 5.5. A BPAY payment is deemed as being received by the biller to whom it is directed no later than the following business day after you direct us to make it.

- 5.6. Notwithstanding this, a delay may occur processing a BPAY payment if a biller, or another financial institution participating in BPAY, does not comply with its BPAY obligations.
- 5.7. Please note in some circumstances a delay may occur in processing a payment or transfer.

## **6. Future-dated BPAY Payments (excluding Osko)**

- 6.1. If you use this option you should be aware that:
- (i) You can arrange for individual BPAY payments to be made on a future date, or at regular ongoing intervals.
  - (ii) You can cancel a future-dated BPAY payment, after you have given the direction but before the payment due date, via Online Banking or by contacting us on 1800 033 139. You cannot stop the BPAY payment on or after that date.
  - (iii) You are responsible for maintaining in the account to be drawn on sufficient cleared funds to cover all future-dated payments (and other drawings) on the day/s you have nominated for payment.
  - (iv) If a future-dated BPAY cannot be processed due to insufficient cleared funds in the nominated account on the due date for payment, we will attempt to make the payment on the following business day. If a future-dated BPAY cannot be processed due to insufficient cleared funds on two successive business days, a dishonour fee will be charged. If a future-dated BPAY cannot be processed due to insufficient cleared funds on two successive business days, on three consecutive occasions, the auto transfer BPAY will be cancelled.
  - (v) You are responsible for checking your account transaction details or account statement/s to ensure that future-dated BPAY payments are made correctly.
  - (vi) You should contact us on 1800 033 139 if there are any problems with your future-dated payment.

## **7. Transaction Limits**

- 7.1. We may limit the amount of payments or transfers you may make on any one day.
- 7.2. If at any time BPAY allows transactions other than bill payments to be processed through BPAY, we will advise accordingly.
- 7.3. We will advise you of applicable transaction limits.

## **8. Refusing Transaction Directions**

- 8.1. You acknowledge and agree that:
  - (i) We may refuse for any reason to give effect to any request or direction you give us in respect of a transaction.
  - (ii) We are not liable to you or any other person for any loss or damage which you or that other person may suffer as a result of such refusal.
  - (iii) If an account from which the payment or transfer is to be made has insufficient cleared funds, we may dishonour the payment or transfer direction (and you may be charged a dishonour fee). We may set off your liabilities against any other account you have with us but this does not affect our rights to dishonour the payment or transfer request or direction.

## **9. Your Liability for Electronic Banking Payments and Transfers**

- 9.1. You are liable for all transactions on your account carried out via Online Banking, Mobile Banking and Telephone Banking including BPAY, by you or by anybody carrying out a transaction with your consent, regardless of when the transaction is processed to your account with us.
- 9.2. Your liability for losses arising from unauthorised transactions on your account depends on whether you or anybody using passwords with your consent contributed to the loss. For the purposes of this condition, the expression 'you' includes anybody using passwords with your consent. You contribute to the losses by any of the following (as well as in other ways):
  - (i) Disclosing your passwords to any person including your joint membership holder, a family member or friend;

- (ii) Recording your passwords on your card or without making a reasonable attempt to disguise them;
- (iii) Selecting passwords such as your or other's name, date of birth or personal details that can easily be identified;
- (iv) Allowing any person to watch you or overhear you using your passwords;
- (v) Failing to protect the security of the passwords by any other act recognised by any court, government agency or industry ombudsman as a serious act contributing to the loss; and
- (vi) Unreasonably delaying the notification of the security breach in respect of the passwords. If you cannot memorise your passwords and must record them, then do not under any circumstances:
  - > Record your passwords in an obvious place as a password, unless you have taken reasonable steps to disguise your passwords carefully. (It is not reasonable to disguise your passwords as a telephone number, a birth date or by changing the order of the characters in the passwords)
  - > Change your passwords to PINs generated by a non-financial institution.
- (vii) Leaving your mobile phone, mobile device, PC or access device logged into Online Banking or Mobile Banking.
- (viii) Storing your User ID or Password on your mobile phone, mobile device, PC or access device.

9.3. If you contributed to the losses, you are liable for actual losses arising from unauthorised transactions incurred during the relevant times\* except:

- (i) As set out in conditions 9.5 and 9.6 and/or
- (ii) To the extent that the actual losses exceed the amounts you could lawfully have accessed from your account at the relevant times\*, having regard to daily transaction limits, the account balance and any pre-arranged credit.

\* The relevant times for these purposes are:

- > In respect of conditions 9.2 (i) - (v): any time prior to reporting the loss or theft or unauthorised use or security breach in accordance with condition 3 – Security Breaches
  - > In respect of condition 9.2 (vi): the time from when you became aware of the loss or theft or unauthorised use or security breach (or should reasonably have become aware of any loss or theft of the card or unauthorised use) and the time when this was reported.
- 9.4. If it is not clear whether you contributed to the loss, your liability in respect of unauthorised transactions, is the lesser of:
- (i) The actual losses prior to you reporting the loss or theft or unauthorised use or security breach
  - (ii) \$150.00; or
  - (iii) The balance in the affected account (including any prearranged credit limit).
- 9.5. You are not liable for losses arising from transactions if these transactions are the result of:
- (i) Fraudulent or negligent conduct of employees or agents of any organisation (including us and any biller)
  - (ii) The use of a password, a card or details from a card which is forged, faulty expired or cancelled (as applicable)
  - (iii) Completing a transaction accepted otherwise than in accordance with your instructions
  - (iv) A payment or transfer being debited more than once to your account
  - (v) A payment or transfer effected prior to you receiving your password.
- 9.6. You will also not be liable for any unauthorised Electronic Banking transaction if:
- (i) It was made after your report to us of the loss or theft or unauthorised use or breach of security or password; or
  - (ii) It can be shown that you did not contribute to any unauthorised transaction made prior to your report of the loss or theft or unauthorised use or breach of security or passwords.

## **10. Our Liability in Respect of Online Banking, Mobile Banking and Telephone Banking**

- 10.1. This section applies to Online Banking, Mobile Banking and Telephone Banking
- 10.2. You agree that subject to your rights which are implied by law and which cannot be excluded by these Terms and Conditions, we will not be liable for:
- (i) Any breakdown or interruption in the system due to circumstances which are not under our direct control
  - (ii) Any corruption of data or any breakdown or interruption to your computer or any other equipment utilised to access Online Banking, Mobile Banking and Telephone Banking
  - (iii) Any error or delay in the execution of any Electronic Banking transaction instructions you provided if the error or delay is due to circumstances not under our direct control; or
  - (iv) Any refusal of another party to receive any Electronic Banking payment from you.
- 10.3. You agree that in the event of a breakdown or interruption to the system or any failure or error in any transmission of information in respect of Online Banking, Mobile Banking and Telephone Banking, we will not be liable for any resulting loss except that we will:
- (i) Reverse any erroneous entry to your account caused by the malfunction
  - (ii) Refund any charges or fees imposed as a result; and
  - (iii) Re-transmit any information and/or repeat any interrupted service or process, as appropriate.
- 10.4. You agree that in any event, our liability to you in respect of any Online Banking, Mobile Banking and Telephone Banking transaction or for your use of Online Banking, Mobile Banking and Telephone Banking does not include consequential, indirect or economic loss.

## **11. Resolving Errors on Account Statements**

- 11.1. All relevant transactions and applicable fees will be recorded on the account statements of the accounts to which they are debited.
- 11.2. If you believe a transaction entered on your statement is wrong, contact us and give the following details:
  - (i) Your name and account number
  - (ii) The date and amount of the transaction in question
  - (iii) The date of the account statement in which the transaction in question first appeared
  - (iv) A brief and clear explanation of why you believe the transaction is unauthorised or an error.
- 11.3. If we are unable to settle your concern immediately and to your satisfaction, we will advise you in writing of the procedures for further investigation and resolution of the complaint and may request further relevant details from you.
- 11.4. After we have received from you details of your complaint, we will do any of the following:
  - (i) Advise you in writing of the results of our investigation; or
  - (ii) Advise you in writing that we require further information to complete our investigation.
- 11.5. In exceptional circumstances, which must be advised in writing, we may require more time to complete our investigation. In such circumstances we will provide you with monthly updates on the progress of the investigation and its likely resolution date, except where we are waiting for a response from you and you have been advised that we require such a response.
- 11.6. If we find that an error was made, we will make the appropriate adjustments to your affected account, including interest and charges (if any) and will advise you in writing of the amount of the adjustment.
- 11.7. When we advise you of the outcome of our investigation, we will give you reasons for our decision by reference to these Terms and Conditions. We will advise you of any adjustments we made to your affected account and also advise you in writing



of other avenues of dispute resolution. You may use these avenues of dispute resolution if you are not satisfied with our decision.

- 11.8. If we decide that you are liable for all or any part of a loss arising out of an unauthorised transaction, we will:
- (i) Give you copies of any documents or other evidence we relied upon in reaching this decision; and
  - (ii) Advise you whether or not there was any system malfunction at the time of the transaction complained of.
- 11.9. If we fail to carry out these procedures or cause unreasonable delay, we will be liable for the amount of the disputed transaction if our failure or delay has prejudiced the outcome of the investigation.

## **12. Transaction Recording**

It is recommended that you record all receipt numbers issued in respect of transactions to assist in checking transactions against your statements.

We recommend you record the receipt numbers on the relevant bills.

## **13. Transaction and Other Fees**

- 13.1. We will advise whether we charge any fees, and the amount of such fees (including any dishonour fee), for:
- (i) Any transaction; or
  - (ii) Giving you access to Electronic Banking; or
  - (iii) Any other service provided in relation to Electronic Banking.
- 13.2. We will also advise whether we will debit to you government charges, duties or taxes arising out of an Electronic Banking transaction.
- 13.3. We may charge a dishonour fee/s for any cheques, transfers, payments or future-dated payments not made due to insufficient cleared funds being held in the relevant account.

## **14. Changes to Terms and Conditions**

- 14.1. We may change these Terms and Conditions and any fees and charges from time to time.

- 14.2. We will notify you in writing, or where authorised, electronically at least 30 days before the effective date of change or such other longer period as may be required by law if the change to the Terms and Conditions will:
- (i) Impose or increase charges for Electronic Banking transactions; or
  - (ii) Increase your liability for unauthorised use; or
  - (iii) Make any changes to your account(s) in respect of which the law requires that notice be given to you.
- 14.3. If you do not wish your daily limit on transacted amounts via Electronic Banking to be changed you must notify us before the effective date of change. Otherwise, once you access the changed transaction limit, you will be deemed to have consented to the change.
- 14.4. We may notify you of other changes by:
- (i) Notices on, or with, periodic account statements
  - (ii) Direct written notice to you or where authorised electronically;
  - (iii) Notices posted on our website; or
  - (iv) Press advertisements in national or local media.
- 14.5. We are not obliged to give you advance notice if an immediate change to the Terms and Conditions is deemed necessary by us for security reasons.
- 14.6. We are not obliged to give you advance notice if a variation involving an interest rate, fee or charge will result in a reduction in your obligations.
- 14.7. BPAY and Osko are owned and operated by third parties. If the rules and regulations of is BPAY or Osko require that these Terms and Conditions be changed, in any way at any time, (including without prior or full notice to you) then we will have the right to change these Terms and Conditions accordingly.

## **15. Cancellation of Electronic Banking Access**

This section applies to Online Banking, Mobile Banking and Telephone Banking.

- 15.1. You may cancel your access at any time by giving us written notice.

15.2. Your access will be terminated when:

- (i) We notify you that your account has been cancelled;
- (ii) You close the last of your accounts with us which has access;
- (iii) You cease to be our member;
- (iv) You alter the account signing authority/s governing the use of your account or accounts which results in current users no longer being authorised to transact (unless we agree otherwise).

15.3. In addition, we may cancel your access at any time. Should this occur, we will provide you with written notice. This notice does not need to provide reasons for cancellation.

## Section 1A - Osko Payments

### 1. General

- 1.1 These terms and conditions apply when you use Osko to make payments from a *linked account* or utilise other facilities made available by us through Osko from time to time.
- 1.2 Osko is a product offered by BPAY and the BPAY scheme governs the way in which we provide *Osko services* to you. However, an *Osko payment* is not a BPAY payment.
- 1.3 We are authorised to provide *Osko services* to you.
- 1.4 Italicised words have a special meaning, as explained at the end of these *Osko terms* and/or at the start of this DPS.

### 2. Applicable Terms and Conditions

- 2.1 These *Osko terms* are additional terms and conditions that apply to your *linked account* when you use *Osko services* via your *linked account*.
- 2.2 The general account terms of your *linked account* referred to in this DPS and elsewhere continue to apply when you use *Osko services* via your *linked account*.
- 2.3 You agree to these *Osko terms* when you first use *Osko services* via your *linked account*.

2.4 To the extent of any inconsistency between the general account terms of your *linked account* referred to in this DPS and these *Osko terms*, these *Osko terms* prevail.

### **3. Osko Services**

3.1 The *Osko service* we currently offer is a payment service, which allows customers to make and receive *Osko payments* in near real time.

3.2 We may offer other *Osko services* to you from time to time.

3.3 We may suspend or discontinue any or all *Osko services*.

3.4 Notices may be published, including by posting to our website, or through direct communication with you.

3.5 If we are no longer able to offer you *Osko services* you will not be able to send or receive *Osko payments* through us.

3.6 Where we are able to do so, we will tell you:

(a) if there are any delays in processing *Osko payments*;

(b) when an *Osko payment* is likely to be completed; and

(c) give you the opportunity to cancel an *Osko payment* if it is delayed.

### **4. How to Use Osko**

4.1 *Osko payments* can be sent from and be made to those savings accounts specified in the Electronic Banking Transaction Products Matrix.

4.2 Where available, *Osko payments* will be presented as a payment option on our electronic banking service channels and the *linked account* through which *Osko payments* are available.

### **5. How Osko Payments Work**

5.1 You can make an *Osko payment* to another person provided that the account of the person you are paying is enabled to receive *Osko payments*.

5.2 Some payees might not be able to receive *Osko payments*. Your ability to make an *Osko payment* to another person depends on their account type and their financial institution.

- 5.3 To make an *Osko payment* to another person, you need to either specify a PayID or the BSB/Account number of that other person, along with other information we require.
- 5.4 If the account associated with the PayID or Account number you enter when seeking to make an *Osko payment* to another person does not accept *Osko payments*, we will notify you.
- 5.5 Using Osko, currently you can only make immediate payment.
- 5.6 You should ensure that all information you provide when requesting an *Osko payment* is correct as we will not be able to cancel an *Osko payment* once it has been made.

## **6. Transaction Limits**

- 6.1 We may impose limits on the individual and aggregate value of *Osko payments* permitted.
- 6.2 These limits may be different from limits that apply to other payment types.
- 6.3 These limits will be notified to you from time to time.

## **7. Fees and Charges**

Fees and charges relating to use of *Osko payments* may apply and are detailed in the Fees and Charges Schedule as amended from time to time.

## **8. Notifications**

- 8.1 Notices to you will be given in accordance with the provisions of the DPS.
- 8.2 Notification of *Osko payments* made or requested will be notified to you via your preferred communication channel.

## **9. Liability**

- 9.1 The provisions of Part 4, Section 1 (Payment Facilities and Services Electronic Banking) of this DPS apply to *Osko payments* made and received to the extent that they are not inconsistent with these *Osko terms*.
- 9.2 The provisions of this DPS dealing with *mistaken internet payments* apply to *Osko payments* you make.
- 9.3 The provisions of this DPS dealing with mistaken internet deposits apply to *Osko payments* you receive.

## **10. Suspension and Termination**

- 10.1 We may suspend your ability to make *Osko payments* at any time where we believe on reasonable grounds that it is necessary to do so to prevent loss to us or *you*, including where we suspect that the service is being used or will be used for fraud or fraudulent purposes or for purposes contrary to applicable legislation.
- 10.2 We may suspend or cancel *your* ability to make *Osko payments* at any time for any reason. The notice does not have to specify a reason for the suspension or cancellation.
- 10.3 *Osko services* may be temporarily unavailable when system maintenance or upgrades are performed.
- 10.4 We will be required to terminate the *Osko service* if *our* membership of BPAY or our participation in Osko is suspended, ceases or is cancelled. We will provide *you* with as much notice as possible if this occurs.
- 10.5 We may also suspend or terminate our offering of any *Osko services* to you if you breach any obligation under these *Osko terms* and fail to remedy the breach where such breach is capable of being remedied upon request you do so.

## **11. Privacy and Confidentiality**

- 11.1 In order to provide you with *Osko services*, we may need to disclose *your* personal information to BPAY and/or its service providers.
- 11.2 If we do not disclose *your* personal information to BPAY or its service providers, we may not be able to provide *you* with *Osko services*.
- 11.3 *You* agree to *us* disclosing to BPAY, its service providers and such other participants involved in Osko such personal information relating to *you* as is necessary in order for *us* to facilitate the provision of *Osko services* to you.

## **12. Changes to Terms and Conditions**

We may change these *Osko terms* from time to time in accordance with the procedure set out in this DPS.

*You* may terminate *your* participation in Osko by written notice to us.

### 13. Definitions

For the purposes of these *Osko terms* the following definitions apply in addition to the definitions set out at the start of this DPS:

**Linked account** – any of *your accounts* which are enabled to make and receive *Osko payments*.

**Osko payment(s)** – a payment made by you or on *your* behalf to a *payee* using Osko.

**Osko service(s)** – a payment service which allows customers to make and receive *Osko payments* in near real time utilising the NPP and such other services which may be offered to *you* via Osko from time to time.

**Payee** – means a person to whom *you* make an *Osko payment*.

## Section 2 – Mistaken Internet Payments

1. This section applies where you make a mistaken internet payment through a “pay anyone” internet banking facility, (including via Osko) but does not include payments made using BPAY. For payments using BPAY please refer to conditions 5 and 6 of Section 1.
2. This condition only applies where the receiving ADI subscribes to the ePayments Code. If the receiving ADI is not a subscriber to the ePayments Code, we will be unable to seek recovery of a mistaken internet payment made to an unintended recipient.
3. You are liable for all payments made using a “pay anyone” internet banking facility, but we will seek to recover funds from an unintended recipient as a result of a mistaken internet payment in the circumstances set out in this section.
4. In this section we explain the circumstances in which we will seek to recover funds on your behalf from an unintended recipient, and the circumstances in which you will be liable for losses arising from a mistaken internet payment.
5. It is important when using an internet banking facility to make a payment that you use the correct identifiers. (including PayID where applicable).

6. You need to be aware that when you make a payment using a 'pay anyone' facility:
  - 6.1. Your funds may be credited to an account of an unintended recipient if the BSB and other identifiers you use do not belong to the named recipient; and
  - 6.2. It may not be possible for us to recover funds from an unintended recipient.
7. When you discover a mistaken internet payment has been made, you need to notify us as soon as you become aware of that fact.
8. To notify us and report a mistaken internet payment please contact us:
  - > By telephone on (03) 8624 5888 or 1800 033 139 between 8am and 8pm, on business days (AEST).
  - > By facsimile on (03) 8624 5892
  - > By email to:  
info@defencebank.com.au
  - > Via our website at:  
defencebank.com.au
  - > By mail to our Registered Office at:  
Defence Bank  
PO Box 14537  
Melbourne VIC 8001
9. When you report a mistaken internet payment we will investigate the matter, contact the receiving ADI and satisfy ourselves that:
  - 9.1. a mistaken internet payment has occurred; and
  - 9.2. there are sufficient funds available in the account of the unintended recipient to the value of the mistaken internet payment.
10. What then happens depends on how long after the mistaken internet payment was made you reported the matter to us. The relevant periods are:
  - > Within 10 business days of the payment
  - > Between 10 business days and 7 months after the payment
  - > More than 7 months after the payment.



11. Where you report a mistaken internet payment within 10 business days of the payment being made, then, after satisfying ourselves as to the matters set out in condition 9, Section 2 (Part 4):

11.1. We will send the receiving ADI a request for return of the funds, and

- (i) If the receiving ADI is satisfied that a mistaken internet payment has occurred and there are still sufficient funds in the account of the unintended recipient, then the receiving ADI is under an obligation under the ePayments Code to return the funds to us within 10 business days of receiving our request; or
- (ii) If the receiving ADI is not satisfied that a mistaken internet payment has occurred, the receiving ADI may still seek, but is not obliged to seek, the consent of the unintended recipient to return the funds to us.

11.2. When we receive any returned funds from the receiving ADI we will credit your relevant account as soon as practicable.

12. Where you report a mistaken internet payment between 10 business days and 7 months after making the payment, then, after satisfying ourselves as to the matters set out in condition 9, Section 2 (Part 4):

12.1. We will send the receiving ADI a request for a return of the funds, and

12.2. The receiving ADI is obligated under the ePayments Code to investigate the reported mistaken internet payment within 10 business days of receiving our request; and

12.3. If the receiving ADI is satisfied that a mistaken Internet payment has occurred and there are sufficient funds in the account of the unintended recipient, then the receiving ADI must:

- (i) Prevent the unintended recipient from withdrawing the funds from their account for a further 10 business days; and

- (ii) Notify the intended recipient that the receiving ADI will itself withdraw the funds from their account if the unintended recipient does not establish an entitlement to those funds within the period of 10 business days; and
- (iii) If the unintended recipient does not establish an entitlement to the funds within 10 business days the receiving ADI is obliged, under the ePayments Code, to return the funds to us; or

12.4. If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may still seek, but is not obliged to seek, the consent of the unintended recipient for return of the funds to us;

12.5. When we receive any returned funds from the receiving ADI we will credit your relevant account as soon as practicable.

13. Where you report a mistaken internet payment more than 7 months after making the payment, then, after satisfying ourselves as to the matters set out in condition 9, Section 2 (Part 4):

13.1. We will send the receiving ADI a request for a return of the funds, and

- (i) If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must, under the ePayments Code, seek the consent of the unintended recipient to return of the funds; or
- (ii) If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may still seek, but is not obliged to seek, the consent of the unintended recipient for return of the funds to us; and

13.2. When we receive any returned funds from the receiving ADI we will credit your relevant account as soon as possible.

14. Where in condition 13.1(i) as above the receiving ADI seeks the consent of the unintended recipient for return of the funds, but the unintended recipient does not so consent or respond the receiving ADI has no further obligations in the matter.
15. In circumstances where the unintended recipient of a mistaken internet payment is receiving income support payments from Centrelink, the receiving ADI must recover the funds from the unintended recipient in accordance with the Code of Operation for Centrelink Direct Credit Payments, which means that recovery may have to be made by instalments with certain minimum protective amounts. Where this circumstance occurs we will notify you.
16. In circumstances where both ourselves and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient funds available in the account of the unintended recipient to the full value of the mistaken internet payment, then, except in the circumstances contemplated in condition 14 (as above), the receiving ADI must use its reasonable endeavours to retrieve the funds from the unintended recipient for return to us, which may involve arranging with the unintended recipient for repayment by instalments.
17. We will inform you in writing of the outcome of your report of a mistaken internet payment within 30 business days of the day on which you make the report.
18. If you are not satisfied with the manner in which your report about a mistaken internet payment has been dealt with either by ourselves or the receiving ADI you may lodge a complaint. We must deal with that complaint in accordance with our internal dispute resolution procedures and if you are not satisfied, you may refer the matter to our External Dispute Resolution Scheme.

## Section 3 – Other Payment Facilities and Services

### Payment Services Matrix

The following matrix sets out the availability of payment services by savings account type:

| Payment Services          |             |              |               |                             |             |
|---------------------------|-------------|--------------|---------------|-----------------------------|-------------|
| Account Type              | Cheque book | Direct Debit | Direct Credit | Electronic Banking Transfer | OSKO/ PayID |
| Basic Access              | X           | ✓            | ✓             | ✓                           | ✓           |
| Budget Savings            | X           | ✓            | ✓             | ✓                           | ✓           |
| Cadet Saver               | X           | ✓            | ✓             | ✓                           | ✓           |
| Cash Management           | X           | ✓            | ✓             | ✓                           | ✓           |
| Christmas Savings         | X           | ✓            | ✓             | ✓                           | ✓           |
| Everyday Access           | ✓           | ✓            | ✓             | ✓                           | ✓           |
| Flexi Term                | X           | ✓            | ✓             | ✓                           | ✓           |
| General Insurance Savings | X           | ✓            | ✓             | ✓                           | ✓           |
| Investment Savings        | X           | ✓            | ✓             | ✓                           | ✓           |
| iSaver                    | X           | ✓            | ✓             | ✓                           | ✓           |
| Kids Club Savings         | X           | X            | ✓             | X                           | X           |
| Max eSaver                | X           | ✓            | ✓             | ✓                           | ✓           |
| National Access           | ✓           | ✓            | ✓             | ✓                           | ✓           |
| Offset                    | ✓           | ✓            | ✓             | ✓                           | ✓           |
| Pension Saver             | ✓           | ✓            | ✓             | ✓                           | ✓           |
| Reservist Saver           | ✓           | ✓            | ✓             | ✓                           | ✓           |
| Salary Saver              | ✓           | ✓            | ✓             | ✓                           | ✓           |
| Teen Saver                | X           | ✓            | ✓             | ✓                           | ✓           |

### Fees and Charges

The fees and charges for these payment services are detailed in the Fees and Charges Schedule.

The Fees and Charges Schedule and our brochure titled 'Tips for reducing your banking fees with Defence Bank' are available at your nearest Defence Bank branch, by visiting [defencebank.com.au](http://defencebank.com.au) or by calling 1800 033 139.

## Government Charges

We will debit your savings account with any applicable government charges as a result of using a payment service including any government charges introduced after the facility is established.

## Specific Terms and Conditions

### 1. Direct Debits

- 1.1 By signing and providing a biller with a direct debit request you authorise the biller to have funds debited from your account with Defence Bank.
- 1.2 We are not advised by the biller when a direct debit request is established or discontinued.
- 1.3 Acting on the authority of an electronic file received from the biller's financial institution, we will debit the nominated account and transfer funds in accordance with instruction received from the biller's financial institution.
- 1.4 We accept no responsibility for the date on the instruction received from the biller's financial institution and the date on which the debit is processed to the nominated account.
- 1.5 Any instruction received for payment on a non-business day will be processed and payment made on the next business day.
- 1.6 Stopping a direct debit:
  - (i) We will promptly stop a direct debit facility linked to your transaction account with us whenever you ask us to do so by advising us in writing. We recommend that, you also advise the biller that you wish to cancel the direct debit.
  - (ii) If you wish to stop a direct debit from your debit or credit card you will need to advise the biller directly.
- 1.7 Direct debit requests received by us will be debited from the account nominated by the biller or as directed by you in writing to us. If there are insufficient funds in the nominated account, we will dishonour the debit and advise the biller that there were insufficient funds.

- 1.8 If on the first presentation of a new direct debit you have only nominated your membership number with a biller, we will debit your Everyday Access account. If there are insufficient funds in your Everyday Access account, we will debit, and you authorise us to debit, the amount from the following accounts in the order in which they appear: Everyday Access, National Access, Offset, Salary Saver, Budget Savings, General Insurance Savings, iSaver, Basic Access, Max eSaver, Reservist Saver, Cadet Saver, Teen Saver. Should there be insufficient funds in any of these accounts we will dishonour the debit and advise the biller that there were insufficient funds.
- 1.9 A dishonour fee is payable if there are insufficient funds in the Everyday Access account (or other account detailed in 1.8 above) and any other nominated account when we receive the direct debit instruction.
- 1.10 In certain circumstances we will exercise our discretion and honour a direct debit request in situations where there are insufficient funds to cover the debit. Where this action results in the account becoming overdrawn a direct debit honour fee is payable as set out in the Fees and Charges Schedule.

## **2. Direct Credits**

- 2.1 We are not advised when a direct credit authority is established or discontinued by you with a third party. We will credit the nominated account on the authority of an electronic file received from the crediting party's financial institution.
- 2.2 We accept no responsibility for the date on which the instruction is received from the crediting party's financial institution and the date on which the credit is processed and made to the nominated account. Any instruction received for crediting on a non business day will be processed and the payment credited on the next business day.
- 2.3 We will not accept any request to cancel a direct credit facility or stop an individual direct credit. Any such request must be directed to the crediting party before the instruction is received by us.
- 2.4 If we receive a request from a crediting party to reverse an amount previously credited, resulting in your

account becoming overdrawn, then the overdrawn balance becomes payable by you immediately.

### **3. Auto Transfers**

- 3.1 External auto transfers are only available to financial institutions with a BSB number.
- 3.2 Financial institutions receive auto transfers as cleared funds on the next business day.
- 3.3 While we will endeavour to process an auto transfer in accordance with your instructions, we accept no responsibility if any such transfer is not or cannot be made and accordingly shall not incur any liability through our refusal or omission to make any or all of the payments instructed by you or arising from any late payment, omission or failure on our part.
- 3.4 If an auto transfer cannot be processed due to insufficient cleared funds in the nominated account on the due date for payment, we will attempt to make the payment on the following business day. If an auto transfer cannot be processed due to insufficient cleared funds on two successive business days, a dishonour fee will be charged. If an auto transfer cannot be processed due to insufficient cleared funds on two successive business days, on three consecutive occasions, the auto transfer will be cancelled.
- 3.5 We may in our absolute discretion conclusively determine the order of priority of payment by us under this facility and any authority given to us by the member.
- 3.6 Where you make an external auto transfer through a 'pay anyone' internet banking facility the provisions dealing with *mistaken internet payments* apply to that transfer.

### **4. Member Chequing**

#### 4.1. Access

The Member Chequing facility can only be attached to a National Access, Everyday Access, Salary Saver, Reservist Saver, Offset and Pension Saver account or a Smart Mover loan.

#### 4.2 Authority

By acquiring a Member Chequing facility you acknowledge and authorise Defence Bank to debit

your account for:

- > The amount of any dishonour charges imposed by Defence Bank
- > The amount of any government taxes or duties in respect of transactions or the operation of the account
- > The amount of any other fees and charges payable under these Terms and Conditions.

#### 4.3 Dishonouring a Cheque

If the amount of any cheque presented for payment exceeds the available balance (including uncleared cheque(s) deposits, available credit or unused overdraft facility) in your Defence Bank account at the time the cheque is presented we may instruct the presenting bank to refuse to pay the cheque. Where we refuse to pay a cheque in accordance with this condition or in accordance with any other provision, we may at our absolute discretion, debit your Defence Bank account with any costs incurred through such refusal and such costs shall constitute a debt from you to Defence Bank.

In the event that a correctly authorised and presented cheque exceeds the available balance of your Defence Bank account, we are authorised to transfer to that account, (from any other account or accounts held by you with Defence Bank) sufficient funds to allow payment of the cheque. If there are insufficient funds and the presented cheque is honoured by us, the amount in excess of the available balance shall be a debt immediately payable to us. If subsequent to written demand by us, you fail to repay the debt, you will be liable to pay all costs and expenses incurred by Defence Bank in the collection of that debt.

#### 4.4 Stopping a Cheque

If it is necessary for you to request that payment of any cheque be stopped you must provide a signed stop payment notice to us.

Where we agree to your request to stop payment, you agree to indemnify Defence Bank against any loss we may suffer or be liable to suffer as a result of the stop payment. You also agree to indemnify Defence Bank against cost of any litigation that may be brought against us by any person as a result of



payment being stopped at your request.

#### 4.5 Security of Your Cheque Book

It is your responsibility to safeguard your cheque book from loss, theft or unauthorised use.

You must:

- > Keep your cheque book under secure control and in a safe place at all times
- > Never give your cheque book or an incomplete cheque to any person
- > Read your periodic statement carefully and notify us promptly if it contains any entry which you suspect may represent an unauthorised transaction and
- > Contact us immediately if you become aware that your cheque book or a cheque has been lost, stolen or used without your authority. You will be liable for any loss arising from a failure to report the loss, theft or misuse of your cheque book.

#### 4.6 Cheque Clearance

Generally it will take 3 business days to clear a cheque. Exceptions to this are foreign cheques.

Foreign cheques less than \$AUD25,000 will require a 60 day clearance period.

Funds from foreign cheques of \$AUD25,000 or more will be available upon clearance from the overseas bank on which the cheque is drawn.

Despite the above clearance having been granted, an overseas cheque dishonour may still occur several months later.

In the event that a foreign cheque is returned unpaid, we will debit your account with the Australian dollar value of the foreign cheque, using the exchange rate current at the time the cheque is dishonoured.

#### 4.7 Writing Cheques

When you write a cheque you have a duty to fill it out carefully so that no one else can alter it. You must:

- > Write the amount in both words and figures and never leave a gap between the words or figures
- > Begin the amount in words as close to the left hand side of the cheque as possible and write the amount in figures as close as possible to the

dollar (\$) sign

- > Always write cheques in ink which cannot be rubbed out and never in pencil and
- > Never sign a cheque until you have filled it out completely.

#### 4.8 Crossed Cheques

A cheque with two parallel lines across it is a 'crossed cheque'. When you cross a cheque, you are telling the bank that the cheque must be paid into an account and not cashed.

##### (i) 'Not Negotiable' Cheques

The words 'Not Negotiable' between two parallel lines protects the true owner of a lost or stolen cheque. These words do not prevent the cheque being negotiated or transferred to a third party before presentation to a bank or financial institution for payment.

##### (ii) 'Account Payee Only'

If you write these words on a cheque, you are directing the bank collecting the cheque to only pay the cheque into the account of the person named on the cheque.

##### (iii) 'Or Bearer'

These words mean that a bank may pay the cheque to whoever is in possession of the cheque, not only the person named on the cheque. If you delete these words, the cheque becomes an 'or order' cheque.

##### (iv) 'Or Order'

An 'or order' cheque means that if the payee wants to transfer the cheque to another person, they can do so by firstly signing the back of the cheque.

You must delete the words 'or bearer' and replace them with 'or order' to make the cheque an 'or order' cheque.

#### 4.9 Liability

You may be liable for all losses caused by your failure to observe the duties specified in condition 4.5 Security

of Your Cheque Book and Writing Cheques above.

However in no case will you be liable where it is shown, on the balance of probabilities, that the loss was caused by:

- > The fraudulent or negligent conduct of Defence Bank's employees or agents or
- > The same cheque being debited more than once to the same account.

#### 4.10 Cheque Dishonour

A cheque may be dishonoured where –

- > There are insufficient funds in the account of the drawer
- > The cheque is unsigned
- > The cheque is more than 15 months old
- > The cheque is future dated
- > The cheque has been materially altered and the alteration has not been signed
- > There is a legal impediment to payment
- > The cheque has been stopped or
- > The paying bank has been notified of the mental incapacity, bankruptcy or death of the drawer.

We may charge a dishonour fee as set out in the Fees and Charges Schedule.

## **Part 5. Visa Debit Card/ rediCARD Conditions of Use**

### **IMPORTANT**

Before you use the Visa Debit Card/rediCARD, read these Conditions of Use carefully. Use of the Visa Debit Card/rediCARD will be governed by these conditions.

These Conditions of Use unless otherwise advised in writing, replace all Visa Debit Card/rediCARD Conditions of Use previously issued.

You should follow the guidelines as detailed below to protect against unauthorised use of the Visa Debit Card/rediCARD and PIN. These guidelines provide examples of security measures only and will not determine your liability

for any losses resulting from unauthorised EFT transactions. Liability for such transactions will be determined in accordance with condition 17 (Part 5) of these Conditions of Use and the ePayments Code.

## **Guidelines for Ensuring the Security of your Visa Debit Card/rediCARD and PIN**

- > Sign the Visa Debit Card/rediCARD as soon as you receive it
- > Keep the Visa Debit Card/rediCARD in a safe place
- > If you change the PIN, you must not select a PIN that represents your birth date or a recognisable part of your name
- > Never write the PIN on the Visa Debit Card/rediCARD
- > Never write the PIN on anything that is kept with or near the Visa Debit Card/rediCARD
- > Never lend the Visa Debit Card/rediCARD to anybody
- > Never tell or show the PIN to another person
- > Use care to prevent anyone seeing the Visa Debit Card/rediCARD number and PIN being entered at Electronic Equipment
- > Immediately report the loss, theft or unauthorised use of the Visa Debit Card/rediCARD to Defence Bank or to the Cardholder lost and stolen card hotline
- > Keep a record of the Visa Debit Card/rediCARD number and the Cardholder lost and stolen card hotline telephone number for your area with your usual list of emergency telephone numbers
- > Examine your periodical statement immediately upon receiving it to identify and report, as soon as possible, any instances where the Visa Debit Card/rediCARD has been used without your authority; and immediately notify Defence Bank of any change of address.

## 1. Introduction

1.1 These Conditions of Use govern use of a Visa Debit Card/rediCARD to access your linked account(s) at Defence Bank. Each transaction on a linked account is also governed by the Terms and Conditions to which that account is subject. In the event of an inconsistency between these Conditions of Use and the Terms applicable to your linked account(s), these Conditions of Use shall prevail.

## 2. Definitions

In these Terms:

**ATM** means Automatic Teller Machine.

**Card Details** means the information provided on the card and includes, but is not limited to, the card number and expiry date.

**Contactless Purchase** means a transaction made by waving or tapping a card (which is capable of making a contactless purchase) in front of a contactless terminal without having to insert or swipe the card or enter your PIN to authorise the transaction.

**Contactless Terminal** means an electronic device which can be used to make a contactless purchase.

**Cuscal** means Cuscal Limited.

**Day** means a 24-hour period commencing on midnight in Australian Eastern Standard Time or Australian Eastern Daylight Time, as the case may be.

**Easy Pay** is a facility where you may authorise and make a purchase from a merchant using your card only without also having to use an access code or manual signature.

**Easy Pay Purchase** means a purchase from a merchant utilising Easy Pay.

**EFT System** means the shared system under which EFT transactions are processed.

**EFT Terminal** means the electronic equipment, electronic system, communications system or software controlled or provided by or on behalf of Defence Bank or any third party for use with a Visa Debit Card/rediCARD and PIN to conduct an EFT transaction and includes, but is not limited to, an automatic teller machine or point of sale terminal.

**EFT Transaction** means an Electronic Funds Transfer initiated by you or your subsidiary cardholder through Electronic Equipment using a Visa Debit Card/rediCARD

and/or PIN or card details but not requiring a manual signature, and includes a contactless purchase even though those transactions do not require provision of an access code to authorise the transaction.

**Electronic Equipment** includes, but is not limited to, a computer, contactless terminal, television, telephone mobile device, EFT Terminal and ATM.

Linked account means account(s) which you may access using a Visa Debit Card/rediCARD, and includes any overdraft or line of credit attached to that account.

**Merchant** means a retailer or any other provider of goods or services authorised to accept payment via Visa Debit Card/rediCARD.

**PIN** means the Personal Identification Number issued to you or a subsidiary cardholder by Defence Bank which is used by you to authorise a transaction.

**Subsidiary Cardholder** means any person nominated by you to whom we have issued a Visa Debit Card/rediCARD which can be used to access your account(s).

**Visa Debit Card/rediCARD** means the Visa Debit Card/rediCARD issued to you or a subsidiary cardholder by Defence Bank.

### **3. Application of these Terms**

- 3.1 These Conditions of Use apply when the Visa Debit Card/rediCARD is used to carry out an EFT transaction.
- 3.2 We may attach other services to the rediCARD. Please contact us for details.
- 3.3 In accepting a Visa Debit Card/rediCARD from Defence Bank you are obliged to comply with these Conditions of Use.
- 3.4 Unless otherwise required by the context, a singular word includes the plural and vice versa.

### **4. Code of Conduct**

- 4.1 We warrant that we will comply with the requirements of the ePayments Code where that code applies.

### **5. Signing the Visa Debit Card/rediCARD**

- 5.1 You agree to sign your Visa Debit Card/rediCARD immediately upon receiving it and before use. This will assist in preventing fraudulent or unauthorised use of your Visa Debit Card/rediCARD.

- 5.2 You must ensure that your subsidiary cardholder signs the Visa Debit Card/rediCARD issued to them immediately upon receiving it and before use.

## **6. Protecting the PIN**

- 6.1 We will provide a PIN to use the Visa Debit Card/rediCARD with certain Electronic Equipment. You agree to protect this PIN. This will assist in the prevention of fraudulent or unauthorised use of the Visa Debit Card/rediCARD.
- 6.2 You must not tell or show the PIN to another person or allow it to be seen by another person, including your family and friends.
- 6.3 If you change the PIN, you must not select a PIN that represents your birth date or a recognisable part of your name. If you use an obvious PIN such as a name or date you may be liable for any losses which occur as a result of unauthorised use of the PIN before notification to Defence Bank that the PIN has been misused or has become known to someone else.
- 6.4 Do not record the PIN on the Visa Debit Card/rediCARD or keep a record of the PIN on anything which is kept with or near the Visa Debit Card/rediCARD unless reasonable steps have been taken to carefully disguise the PIN or to prevent unauthorised access to that record.

## **7. Using the Visa Debit Card/rediCARD**

- 7.1 The Visa Debit Card/rediCARD may only be used to perform transactions on your linked account(s). Defence Bank will advise you of the accounts, including any credit facility, which you may link to the Visa Debit Card/rediCARD.
- 7.2 We will debit your linked account(s) with the value of all transactions, including sales and cash advance vouchers arising from the use of the Visa Debit Card/rediCARD (including all mail or telephone orders placed by quoting the Visa Debit Card/rediCARD number) and all other EFT transactions, or credit your linked account(s) with the value of all deposit transactions at EFT terminals.
- 7.3 We will advise you from time to time:
- (i) What EFT transactions may be performed using the Visa Debit Card/rediCARD; and

(ii) What EFT terminals of other financial institutions may be used.

- 7.4 Transactions will not necessarily be processed to your linked account on the same day.
- 7.5 If a linked account is in the name of more than one person, then each party to that account will be jointly and individually liable for all EFT transactions to that account.
- 7.6 You will be liable to Defence Bank in relation to EFT transactions processed after you have closed your linked account(s) or after your Defence Bank membership is closed.

## **8. Using the Visa Debit Card Outside Australia**

- 8.1 Use of the Visa Debit Card outside Australia must comply with all exchange control requirements.
- 8.2 You agree to reimburse us for any costs, fees or charges of any nature arising out of your failure to comply with exchange control requirements.
- 8.3 All transactions made overseas using Visa Debit Card will prior to being debited to your account be converted into Australian currency by Visa International or an agent of a principal member of Visa International and calculated at a wholesale market rate selected by Visa from within a range of wholesale rates or the government mandated rate that is in effect one day prior to the Central Processing Date (that is, the date on which Visa processes the transaction).
- 8.4 All transactions made overseas using Visa Debit Card are subject to a currency conversion fee equal to a percentage of the value of the transaction. The currency conversion fee is payable to Cuscal and Defence Bank in our respective capacities of principal member of Visa International or an agent of a principal member of Visa International under which Defence Bank can provide the Visa Debit Card access to its members. The percentage used to calculate the currency conversion fee is set out in the Fees and Charges Schedule and is subject to change from time to time. We will advise you in advance of any such change.
- 8.5 Some merchants impose a surcharge for making an EFT transaction. Once you have confirmed the transaction you will not be able to dispute the



surcharge. The surcharge will, in most cases, appear on your statement as part of the purchase price.

- 8.6 Before travelling overseas, you or your subsidiary cardholder should obtain from Defence Bank the Visa Global Customer Assistance Services hotline number for your country of destination.
- 8.7 You may not be able to make contactless purchases in some overseas countries. Different transaction limits may apply.
- 8.8 If your card is lost, stolen or there is unauthorised use of the card and/or PIN, you should advise the Visa Global Customer Assistance Services immediately.

## **9. Withdrawal and Transaction Limits**

- 9.1 You agree that the Visa Debit Card/rediCARD will not be used to:
  - (i) Overdraw any of your linked account(s); or
  - (ii) Exceed the unused portion of your credit limit under any pre-arranged credit facility such as line of credit or overdraft.
- 9.2 If condition 9.1 is breached, we may:
  - (i) Refuse any subsequent request for payment given; and /or
  - (ii) Charge you a fee as advised to you from time to time.
- 9.3 We may at any time limit the amount of an EFT transaction and will advise you of any such daily or periodic transaction limits at the time of your application for the Visa Debit Card/rediCARD.
- 9.4 You acknowledge that third party organisations including merchants or other financial institutions may impose additional restrictions on the amount of funds that may be withdrawn, paid or transferred.
- 9.5 The current daily withdrawal limit is \$1,000 AUD for PIN generated transactions.
- 9.6 A cash advance cannot be made using a card at a contactless terminal.
- 9.7 The current daily transaction limit for contactless purchases is \$100 AUD for each individual transaction and \$300 AUD in the aggregate or as advised from time to time.

## **10. Authorisations**

- 10.1 You acknowledge and agree that:
- (i) We have the right to deny authorisation for any EFT transaction for any reason; and
  - (ii) We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result of such refusal.

## **11. Account Statements**

- 11.1 We will send you an account statement for the linked account at least every three months. You may request more frequent account statements.
- 11.2 In respect of any linked accounts which have a pre-arranged credit facility attached such as a line of credit or overdraft, we will send you an account statement monthly.
- 11.3 You may request a copy of your account statement at any time.
- 11.4 We may charge a fee for responding to any request by you to provide more frequent account statements or copies of your account statements.
- 11.5 Statements of account can also be viewed using Online Banking and selecting the eStatements function.

## **12. Transaction Slips and Receipts**

- 12.1 It is recommended that you check and retain all transaction slips, receipts and payment or transfer reference numbers issued to you after conducting an EFT transaction, as well as copies of all sales and cash advance vouchers, to assist in checking EFT transactions against your statements.
- 12.2 Where you make a contactless purchase or an Easy Pay purchase the merchant is required to issue you with a receipt for the transaction on request and you should ensure one is offered.
- 12.3 When making a contactless purchase you must check that the correct amount of the purchase is displayed on the contactless terminal or on the merchant's register before using your card to make the purchase.

## **13. Subsidiary Cards**

- 13.1 You may authorise us, if we agree, to issue a subsidiary Visa Debit Card or rediCARD to your

nominee, provided this person is over the age of 18 (unless we agree to a younger age).

- (i) You will be liable for all transactions carried out by the subsidiary cardholder on the Visa Debit Card or rediCARD even after you have cancelled the card
- (ii) We will give the primary and the subsidiary cardholder a PIN
- (iii) The subsidiary cardholder's use of the Visa Debit Card or rediCARD and PIN is governed by the Visa Debit Card/redicARD Conditions of Use section in this DPS
- (iv) You must ensure that each subsidiary cardholder protects their Visa Debit Card or rediCARD and PIN in the same way as these Conditions of Use require you to protect your Visa Debit Card or rediCARD and PIN
- (v) If you instruct us to cancel a subsidiary card in writing, you will not be liable for any losses resulting from continuing (unauthorised) use of the subsidiary card following cancellation, provided you:
  - > Take all reasonable steps to ensure the card(s) is destroyed or returned to us; and
  - > Do not act fraudulently or otherwise cause the loss.

## **14. Renewal of the Visa Debit Card/redicARD**

- 14.1 Unless you are in breach of these Conditions of Use or we deem otherwise for the security of the EFT System or individual accounts, we will automatically provide you and your subsidiary cardholder with a replacement Visa Debit Card/redicARD before the expiry date of the current Visa Debit Card/redicARD or additional Visa Debit Card/redicARD.
- 14.2 If you do not wish to receive a replacement Visa Debit Card/redicARD, either for yourself or for your subsidiary cardholder, you must notify us before the expiration date of the current Visa Debit Card/redicARD. You must give Defence Bank reasonable time beforehand to arrange cancellation of the issue of a replacement Visa Debit Card/redicARD.

## **15. Cancellation and Return of the Visa Debit Card/rediCARD**

- 15.1 The Visa Debit Card/rediCARD always remains the property of Defence Bank.
- 15.2 We can immediately cancel the Visa Debit Card/rediCARD and demand its return at any time with cause or if you breach these Conditions of Use or the Terms and Conditions of your linked accounts. This may include capture of the Visa Debit Card/rediCARD at any EFT terminal.
- 15.3 We may at any time cancel any Visa Debit Card/rediCARD without cause. Except in the circumstances referred to in clause 15.4, we will give you at least 14 days advance notice.
- 15.4 We can immediately cancel any Visa Debit Card/rediCARD and demand its return at any time without giving prior notice:
  - (a) If you breach these Conditions of Use or the Terms and Conditions of your linked accounts or
  - (b) If we believe that use of the card may be involved in a breach of applicable laws or
  - (c) If we believe that use of a card may cause loss to you or us
- 15.5 Cancellation of a card pursuant to the provisions of clause 15.4, may involve a capture of the Visa Debit Card/rediCARD at an EFT terminal.
- 15.6 Where we cancel a card without prior notice pursuant to the provisions of clause 15.4 we will notify you of the cancellation as soon as practicable afterwards. The notice does not have to specify the reasons for the cancellation.
- 15.7 You may cancel your Visa Debit Card/rediCARD or any Visa Debit Card/rediCARD issued to your subsidiary cardholder at any time by giving Defence Bank written notice.
- 15.8 If you or Defence Bank cancel the Visa Debit Card/rediCARD issued to you, any Visa Debit Card/rediCARD issued to your subsidiary cardholder(s) will also be cancelled.
- 15.9 You will be liable for any transactions you or your subsidiary cardholder make using the Visa Debit Card/rediCARD before the Visa Debit Card/rediCARD

is cancelled but which are not posted to your linked account until after cancellation of the Visa Debit Card/rediCARD.

15.10 We may, at any time, cancel the Visa Debit Card/rediCARD and any subsidiary cards if you alter the account signing authority/s on your linked account(s) which results in existing Visa Debit Card/rediCARD and subsidiary card holders no longer being authorised to transact on the account unless we agree otherwise.

## **16. Use After Cancellation or Expiry of the Visa Debit Card/rediCARD**

16.1 You must not use the Visa Debit Card/rediCARD or allow your subsidiary cardholder to use the Visa Debit Card/rediCARD:

(i) Before the valid date or after the expiration date shown on the face of the Visa Debit Card/rediCARD; or

(ii) After the Visa Debit Card/rediCARD has been cancelled.

16.2 You will be liable for any debt incurred through such use whether or not you have closed your linked account(s) at Defence Bank.

## **17. Your Liability in Case the Visa Debit Card or rediCARD is Lost or Stolen or in Case of Unauthorised Use**

17.1 You are liable for all losses caused by unauthorised EFT transactions unless any of the circumstances specified in condition 17.2 apply.

17.2 You are not liable for losses:

(i) Where it is clear that you and your subsidiary cardholder have not contributed to the loss;

(ii) That are caused by the fraudulent or negligent conduct of employees or agents of:

> Defence Bank

> Any organisation involved in the provision of the EFT System or

> Any merchant

relating to a forged, faulty, expired or cancelled Visa Debit Card/rediCARD or PIN.

- (iii) That are caused by the same transaction being incorrectly debited more than once to the same account;
- (iv) That would exceed the amount of your liability to Defence Bank, had we exercised our rights (if any) under the Visa International Rules and Regulations against other parties to those rules and regulations; or
- (v) Resulting from unauthorised use of the Visa Debit Card/rediCARD or PIN:
  - > In relation to an EFT transaction which does not require a PIN authorisation, before receipt of the Visa Debit Card/rediCARD,
  - > In relation to an EFT transaction which requires PIN authorisation, before receipt of the PIN, or
  - > In either case, after notification to Defence Bank in accordance with condition 18 that the Visa Debit Card/rediCARD is being used without authority, that it has been lost or stolen, or that PIN security has been breached.

17.3 You will be liable for any loss of funds arising from any unauthorised EFT transaction using the Visa Debit Card/rediCARD or PIN if the loss occurs before notification to Defence Bank or the Cardholder lost and stolen card hotline that the Visa Debit Card/rediCARD has been misused, lost or stolen or the PIN has become known to someone else and if we prove, on the balance of probabilities, that you or your subsidiary cardholder contributed to the loss through:

- (i) Fraud, failure to look after and keep the PIN secure in accordance with condition 6.2, 6.3 and 6.4, or extreme carelessness in failing to protect the security of the PIN; or
- (ii) Unreasonably delaying notification to Defence Bank or the Cardholder lost and stolen hotline of the misuse, loss; or theft of the Visa Debit Card/rediCARD or of the PIN becoming known to someone else and the loss occurs between the time you or your subsidiary cardholder did, or

reasonably should have, become aware of these matters and the time of notification to Defence Bank or the Cardholder lost and stolen card hotline.

However, you will not be liable for:

- > The portion of the loss that exceeds any applicable daily or periodic transaction limits on your linked account(s),
- > The portion of the loss on any linked account which exceeds the available balance of that linked account (including any prearranged credit), or
- > All losses incurred on any account which you had not agreed with Defence Bank could be accessed using the Visa Debit Card/rediCARD and PIN.

17.4 Where a PIN was required to perform the unauthorised transaction and condition 17.3 does not apply, your liability for any loss of funds arising from an unauthorised transaction using the Visa Debit Card/rediCARD, if the loss occurs before notification to Defence Bank or the Cardholder lost and stolen hotline that the Visa Debit Card/rediCARD has been misused, lost or stolen or the PIN has become known to someone else, is the lesser of:

- (i) \$150.00 AUD
- (ii) The actual loss at the time of notification to Defence Bank or the Cardholder lost and stolen hotline of the misuse, loss or theft of the Visa Debit Card/rediCARD, or of the PIN becoming known to someone else (except that portion of the loss that exceeds any daily or periodic transaction limits applicable to the use of your Visa Debit Card/rediCARD or your linked account); or
- (iii) The balance of your linked account, including any prearranged credit.

17.5 If, in cases not involving EFT transactions, the Visa Debit Card/rediCARD or PIN are used without authority, you are liable for that use before notification to us or the Cardholder lost and stolen card hotline of the unauthorised use, up to your current daily withdrawal limit.

- 17.6 Notwithstanding any of the above provisions, your liability will not exceed your liability under the provisions of the ePayments Code, where that code applies.
- 17.7 You must return your Visa Debit Card/rediCARD and any Visa Debit Card/rediCARD issued to your subsidiary cardholder to Defence Bank when:
- (i) We notify you that we have cancelled the Visa Debit Card/rediCARD.
  - (ii) You close your linked account(s).
  - (iii) You cease to be a member of Defence Bank.
  - (iv) You cancel your Visa Debit Card/rediCARD, any Visa Debit Card/rediCARD issued to your subsidiary cardholder, or both.

## **18. How to Report Loss, Theft or Unauthorised Use of the Visa Debit Card/rediCARD or PIN**

- 18.1 If you or your subsidiary cardholder believe the Visa Debit Card/rediCARD has been misused, lost or stolen or the PIN has become known to someone else, you or your subsidiary cardholder must immediately contact us (if during business hours), or the Cardholder lost and stolen card hotline at any time on its emergency number detailed in condition 18.6 (i)
- 18.2 The Cardholder lost and stolen card hotline or Defence Bank will acknowledge the notification by giving a reference number. Please retain this number as evidence of the date and time of contacting Defence Bank or the Cardholder lost and stolen card hotline.
- 18.3 When contacting the Cardholder lost and stolen card hotline, you or your subsidiary cardholder should confirm the loss or theft as soon as possible with Defence Bank.
- 18.4 The Cardholder lost and stolen card hotline is available 24 hours a day, 7 days a week.
- 18.5 If the Cardholder lost and stolen card hotline is not operating at the time notification is attempted, the loss, theft or unauthorised use must be reported to Defence Bank as soon as possible during business hours or the Cardholder lost and stolen card hotline (when available) whichever is the sooner. If the Cardholder lost and stolen card hotline is not operating at the



time you attempt to call to cancel your card, we will be liable for any losses which:

- (i) Are incurred after you attempt to call and
- (ii) Are due to the failure to cancel.

BUT ONLY if the loss, theft or unauthorised use is reported to us or the Cardholder lost and stolen card hotline within a reasonable time of either becoming available.

- 18.6 If the loss, theft or misuse occurs outside Australia, you or your subsidiary cardholder must notify an organisation displaying the Visa sign and also then confirm the loss, theft or misuse of the card:
- (i) With Defence Bank by telephone or email as soon as possible; or
  - (ii) By telephoning the Visa Global Customer Assistance Services hotline number for the country you are in, which you must obtain from Defence Bank prior to your departure in accordance with condition 8.6 of these Conditions of Use.

**Cardholder lost and stolen card hotline  
1800 648 027 Australia wide, 7 days a week,  
24 hours a day**

## **19. Steps You Must Take to Resolve Errors or Disputed EFT Transactions**

- 19.1 If you believe an EFT transaction is wrong or unauthorised or your periodical statement contains any instances of unauthorised use or errors, immediately notify Defence Bank. You must give us the following information:
- (i) Your name, account number and Visa Debit Card/rediCARD number,
  - (ii) Detail/s of the transaction/s,
  - (iii) A copy of the periodical statement in which the transaction appears,
  - (iv) An explanation as to why you believe it is an unauthorised transaction or error, and
  - (v) the dollar amount of the transaction.

If your complaint is that you did not authorise the transaction, we may ask you or your subsidiary cardholder to provide further information.

- 19.2 Where the EFT transaction which you believe is wrong

or unauthorised is the result of a mistaken Internet payment to an unintended recipient you need to follow the procedures set out in Part 4, Section 2 of this DPS.

- 19.3 We will investigate your complaint, and if we are unable to settle your complaint immediately to our mutual satisfaction, we will advise you in writing of the procedures for further investigation and may request further details from you.
- 19.4 Within 21 days of receipt of the requested detail Defence Bank will:
- (i) Complete our investigation and advise you in writing of the results of our investigation; or
  - (ii) Advise you in writing that we require further time to complete our investigation.

We will complete our investigation within 45 days of receiving your complaint, unless there are exceptional circumstances.

- 19.5 If we are unable to resolve your complaint within 45 days, we will let you know the reasons for the delay.
- 19.6 If we find that an error was made, we will make the appropriate adjustments to your linked account including (where applicable) adjusting interest and reversing charges. Should this be necessary we will advise you in writing.
- 19.7 If we decide that you are liable for all or any part of a loss arising out of unauthorised use of the Visa Debit Card/rediCARD or PIN, we will:
- (i) Give you copies of any documents or other evidence we relied upon; and
  - (ii) Advise you in writing whether or not there was any system or equipment malfunction at the time of the transaction.
- 19.8 If we fail to carry out these procedures or cause unreasonable delay in resolving your complaint, we may be liable for part or all of the amount of the disputed transaction where that failure or delay has prejudiced the outcome of the investigation.
- 19.9 When we advise you of the outcome of our investigations, we will notify you in writing of the reasons for our decision by reference to these Terms and Conditions and the ePayments Code and advise you of any adjustments we have made to your linked

account. If you are not satisfied with the decision and wish to take the matter further, you can contact the dispute resolution body of which Defence Bank is a member:

Credit and Investments Ombudsman

Reply Paid 252

Sydney South NSW 1235

Telephone: 1800 138 422

Facsimile: (02) 9273 8440

Email: [info@cio.org.au](mailto:info@cio.org.au)

Website: [cio.org.au](http://cio.org.au)

## **20. Transaction and Other Fees**

20.1 We will advise you whether we charge a fee, and the amount of such fee, for:

- > Transactions
- > Issuing the Visa Debit Card/rediCARD or any additional or replacement Visa Debit Card/rediCARD
- > Using the Visa Debit Card/rediCARD
- > Issuing the PIN or any additional or replacement PIN
- > Issuing account statements or
- > Any other service provided in relation to the Visa Debit Card/rediCARD.

20.2 We will advise you of government charges, duties or taxes arising out of any transaction debited to your linked account.

## **21. Exclusions of Warranties and Representations**

21.1 We do not warrant that merchants displaying Visa/rediCARD signs or promotional material will accept the Visa Debit Card/rediCARD in payment for goods and services. You should always enquire beforehand before selecting goods or services.

21.2 We do not accept any responsibility should a merchant, bank or other institution displaying Visa/rediCARD signs or promotional material, refuse to accept or honour the Visa Debit Card/rediCARD. We do not warrant that EFT terminals displaying Visa/rediCARD signs or promotional material will accept our Visa Debit Card/rediCARD.

21.3 We are not responsible for any defects in the goods and services acquired by you through the use of the Visa Debit Card/rediCARD. You acknowledge and accept that all complaints about these goods and services must be addressed to the supplier or merchant of those goods and services.

## **22. Malfunction**

22.1 You will not be responsible for any loss you suffer because an EFT terminal accepted an instruction but failed to complete the transaction. If an EFT terminal malfunctions and you or your subsidiary cardholder should have been aware that the EFT terminal was unavailable for use or malfunctioning, we will only be responsible for correcting errors in your linked account and refunding to you any charges or fees imposed on you as a result.

## **23. Changes to Conditions of Use**

23.1 We reserve the right to change these Conditions of Use from time to time.

23.2 We will notify you in writing (or where authorised electronically) at least 30 days before the effective date of change if we:

- (i) Impose or increase charges for the use of the Visa Debit Card/rediCARD and PIN or for issuing additional or replacement Visa Debit Cards/rediCARDS or PINs
- (ii) Increase your liability for losses; or
- (iii) Impose, remove or adjust daily or other periodic transaction limits applying to the use of the Visa Debit Card/rediCARD, PIN, your linked account(s) or electronic equipment.

23.3 We will notify you of other changes no later than the day the change takes effect by advertisement in the national or local media, notice on our website, in a newsletter or statement of account, where authorised electronically or by individual notice sent to you.

23.4 We are not obliged to give you advance notice if an immediate change to the Conditions of Use is deemed necessary for the security of the EFT system or individual accounts.

23.5 By using the Visa Debit Card/rediCARD after

notification of any such changes, you accept those changes and that use of your Visa Debit Card/rediCARD will be subject to those changes.

## **24. Miscellaneous**

- 24.1 You agree that you will promptly notify Defence Bank of any change of address or email for the purpose of any notifications which we are required to send to you.
- 24.2 We will post account statements to your mailing address as held in our records or where authorised electronically.
- 24.3 You can elect to receive statements electronically via Online Banking. To receive eStatements you need to register via Defence Bank Online Banking. Once registered you will no longer receive your statement via the post and will also be able to view any statement outside of the current statement period (classified as a previous statement).
- 24.4 If the Visa Debit Card/rediCARD is issued on a joint account, each party to that account is jointly and individually liable for all transactions on the Visa Debit Card/rediCARD.

# **Part 6. Verified by Visa Terms**

## **IMPORTANT**

The Verified by Visa service is designed to provide you with improved security when your Visa Debit Card is used to make a purchase online. We encourage you to join the growing number of users who enjoy additional security by using the Verified by Visa service and by shopping at participating Verified by Visa online merchants.

The Terms in this Part govern the Verified by Visa service and form the agreement between you and us regarding the use of the service, so please read them carefully.

To participate in the Verified by Visa program, you may be asked to verify personal details held by us in order to complete the transaction. Should your Visa Debit Card have been compromised in any way, please notify us immediately as you may be liable for unauthorised transactions.

### **1. Accepting these Terms**

- 1.1 By completing or attempting to complete a Verified by Visa transaction, you are deemed to accept

these Terms.

- 1.2 You agree to be bound by these Terms each time you use Verified by Visa.

## 2. Definitions

In these Terms:

**account** means your Visa Debit Card account.

**account holder** means the person or persons in whose name the account is held.

**subsidiary cardholder** means a person other than the account holder who has been nominated by an account holder to operate the account by use of a Visa Debit Card.

**participating online merchant** means a retailer or merchant who offers goods or services for sale online, who is a participant in Verified by Visa.

**Verified by Visa** means the online transaction authentication service provided by us (or our nominated service provider).

**Visa Debit Card** means the Visa Debit Card issued to you or a subsidiary cardholder by Defence Bank.

## 3. Application of these Terms

- 3.1 These Terms in this Part apply to the Verified by Visa service and the Verified by Visa transactions conducted on your account.
- 3.2 In addition to these Terms, all other Terms and Conditions that apply to your Visa Debit Card and account ('Account Terms') still apply, including those set out in Part 5. If there is any inconsistency between these Terms and your Account Terms, your Account Terms will apply to the extent of the inconsistency.

## 4. Guidelines for Maintaining the Security of Your Visa Debit Card

- 4.1 In addition to any other requirements in your Account Terms relating to maintaining security of your Visa Debit Card you agree to, use care to prevent anyone seeing the Visa Debit Card details being entered at the time of authentication.

## 5. Using the Verified by Visa Service

- 5.1 You may use Verified by Visa to make purchases online. However, the Verified by Visa service may only be available in connection with participating online

merchants.

- 5.2 When making an online purchase or other transaction for which Verified by Visa applies, you may be asked to provide certain information to us that allows us to validate your identity and verify that you are the cardholder of the specified Visa Debit Card. The information that you provide may be validated against information we hold about you and may be validated against information held by third parties.
- 5.3 If you are unable to provide the requested information to validate your identity, or if the information you provide is inaccurate or incomplete, or if the authentication process otherwise fails, the merchant may not accept your Visa Debit Card or payment for that transaction and you may be unable to complete an online transaction using your Visa Debit Card.
- 5.4 In order to use Verified by Visa, you must have the equipment and software necessary to make a connection to the internet.
- 5.5 In the event you have a question regarding the authentication process or a transaction using your Visa Debit Card, you should contact us.

## **6. Subsidiary Cardholders**

- 6.1 Subject to the Account Terms, you will be liable for all transactions conducted on your account which are undertaken by a subsidiary cardholder.
- 6.2 Subsidiary cardholders may use the Verified by Visa service, but may be required to confirm their identity using the primary account holder's details.

## **7. Termination of Verified by Visa**

- 7.1 We may discontinue, terminate or suspend (permanently or temporarily) the Verified by Visa service, or any part of the Verified by Visa service, without giving you prior notice. We may also change any aspect or functionality of the Verified by Visa service at any time without giving you prior notice.

## **8. Participating Online Merchants**

- 8.1 You will know that an online merchant is a participating online merchant because you will see the Verified by Visa logo and you may be asked to

verify your identity before completing an online transaction with that merchant.

- 8.2 We do not endorse or recommend in any way any participating online merchant.
- 8.3 Your correspondence or business dealings with, or participation in promotions of online stores through Verified by Visa, including payment for and delivery of related goods or services not purchased via Verified by Visa, and any other terms, conditions, warranties or representations associated with such dealings, are solely between you and the online store. Except as otherwise required by law, we have no responsibility or liability whatsoever arising out of or related to those dealings or the online store's goods, services, acts or omissions.

## **9. Exclusion of Liabilities**

- 9.1 Subject to any warranty which is imported into these Terms by law and which cannot be excluded, the Verified by Visa service is provided by us 'as is' without warranty of any kind, either express or implied, including, but not limited to, any implied warranties of merchantability, fitness for a particular purpose, title or non-infringement.
- 9.2 We will not be liable for any damages whatsoever arising out of or in relation to:
- (i) Your use of or access to (or inability to use or access) the Verified by Visa services; or
  - (ii) Any other failure of performance, error, omission, interruption or defect, or any loss or delay in transmission or a transaction.
- 9.3 If you are dissatisfied with any aspect of the Verified by Visa service, your sole and exclusive remedy is to terminate participation in the Verified by Visa transaction or service, as provided in these Terms.

## **10. Your Conduct**

- 10.1 Whilst using the Verified by Visa service and our internet banking services, you agree not to:
- (i) Impersonate any person or entity using the Verified by Visa authentication process;
  - (ii) Upload, post, email or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed



to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment used by the Verified by Visa service or by us;

- (iii) Spam or flood our internet banking service and the Verified by Visa service;
- (iv) Modify, adapt, sub-license, translate, sell, reverse engineer, decompile or disassemble any portion of the Verified by Visa service;
- (v) Remove any copyright, trademark, or other proprietary rights notices contained in the Verified by Visa service;
- (vi) 'frame' or 'mirror' any part of the Verified by Visa service without our prior written authorisation;
- (vii) Use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, 'data mine' or in any way reproduce or circumvent the navigational structure or presentation of the Verified by Visa service;
- (viii) Otherwise interfere with, or disrupt the Verified by Visa service or our internet banking services or servers or networks connected to us or the Verified by Visa service or violate these Terms or any requirements, procedures, policies or regulations in relation to the Verified by Visa service; or
- (ix) Intentionally or unintentionally violate any applicable local, state, national or international laws or regulations relevant or applicable to the Verified by Visa service.

## **11. Your Liability**

- 11.1 Your liability for unauthorised transactions is governed by your Account Terms.
- 11.2 If you breach these Terms, this may affect your liability for unauthorised transactions. If it is determined that you have contributed to the loss, you may be held liable for the transactions notwithstanding that they are unauthorised.
- 11.3 If you suspect that your Visa Debit Card details have become known to someone else or there is a security

concern, you must immediately notify us of such security concern. If you delay in notifying us of the security concern after you knew or ought to have known of the security concern, you may be in breach of these Terms and you may be liable for all transactions on the Visa Debit Card until notification occurs.

- 11.4 For further details as to reporting a breach of card details, refer to your Account Terms.

## **12. Errors**

- 12.1 If you believe a Verified by Visa transaction is wrong or unauthorised or a periodical statement contains any instances of unauthorised use or errors, you should contact us immediately.

## **13. Changes to Terms**

- 13.1 We can change these Terms at any time, and where we are required to do so under any law, we will notify you of the changes.

# **Section 7 - PayID Terms**

## **1. General**

- 1.1 PayID has been developed as part of the New Payments Platform (NPP), an open access infrastructure facilitating the making of fast *payments* in Australia.
- 1.2 PayID is the name of the addressing capability of the NPP, a function that eliminates the need to enter bank Account number and BSB details when *you* make a *payment* to another person's account or when another person makes a *payment* to *your linked account*.
- 1.3 PayID uses recognisable and memorable pieces of information such as mobile telephone numbers and email addresses, instead of *your* Account number and BSB number.
- 1.4 *You* do not have to create or use a PayID for any of *your accounts*. *You* can continue to operate *your accounts* as normal without a PayID, in which case *payments* to be made from or to *your account* will require *your* BSB details and Account number.

## **2. Applicable Terms and Conditions**

- 2.1 These *PayID terms* are additional terms and conditions

that apply to *your linked account* when you create and link a PayID with that account.

- 2.2 The general account terms of *your linked account* referred to in this DPS and elsewhere continue to apply when you link a PayID to an account.
- 2.3 You agree to these *PayID terms* when you apply for a PayID or request that an existing PayID be linked to an *account*.
- 2.4 To the extent of any inconsistency between the general *account* terms of *your linked account* referred to in this DPS and these *PayID terms*, these *PayID terms* prevail.
- 2.5 Italicised words have a special meaning as explained at the end of these *PayID terms* or in this DPS.

### **3. Creating a PayID**

- 3.1 You may create a PayID and link it to an eligible *account*. Our Electronic Banking Transaction Products Matrix specifies which *account* types may have a PayID linked to them.
- 3.2 Once a PayID is created and linked to an *account*, any *payments* made to that PayID will be directed to *your linked account*.
- 3.3 A PayID may only be linked to one *account* at a time, but an *account* may have multiple PayIDs linked to it.
- 3.4 When you request creation of a PayID, you represent and warrant to us that:
  - (a) you own or are otherwise authorised to use the PayID;
  - (b) the PayID is current, accurate and complete; and
  - (c) we are authorised to register your PayID with the *PayID service*.
- 3.5 We may refuse a request by you to create a PayID where:
  - (a) we have not yet completed verifying or are unable to verify your identity;
  - (b) we are not satisfied that you own or are otherwise authorised to use that PayID;
  - (c) we reasonably suspect that the PayID is or has been or will be used for a fraudulent or illegal purpose;

- (d) we are required to so by law or by the operator of the NPP;
- (e) the PayID requested by *you* is already registered with the *PayID service*.

#### **4. Duplicated PayID**

Where *your* attempt to create a PayID is unsuccessful because that PayID has already been registered by someone else with the *PayID service* (duplicated PayID) then, upon request by *you*, we will provide *you* with reasonable assistance to resolve the issue of the duplicated PayID by contacting the financial institution or other entity that registered the duplicated PayID with the *PayID service*.

#### **5. PayID Name**

- 5.1 To register *your* PayID with the *PayID service*, we are also required to register a *PayID name* to be associated with *your* PayID. When you create *your* PayID, we will either:
  - (a) issue *you* with a *PayID name*; or
  - (b) enable *you* to select *your* own *PayID name* from a list provided to *you*.
- 5.2 We will not permit *you* to select or maintain registration of a *PayID name* that we consider could mislead or deceive a person into sending *you* a *payment* intended for another person.

#### **6. Making Payments to a PayID**

- 6.1 *You* must enter the PayID of the other person as *payee* of the transaction.
- 6.2 We will verify that the PayID *you* have provided to *us* has been registered with the *PayID service* and, where registered, we will inform *you* of the *PayID name* attached to that PayID.
- 6.3 *You* must check to make sure that the *PayID name* displayed matches the identity of the person *you* intend to pay.
- 6.4 If *you* do not recognise the *PayID name* or the *PayID name* does not match the identity of the person *you* wish to pay, then *you* should contact the person *you* wish to pay to confirm that all details are correct before proceeding to make the *payment*.
- 6.5 Use by *you* of incorrect details could result in a *payment* being made to a person other than the person *you*

intend to pay and may result in loss of *your* funds.

## **7. Payments to Your PayID**

The ability of a person to make a *payment* to *your* PayID depends on that person's financial institution, their *account* type and on the type of *payment* to be made. In some cases, the other person may not be able to make a *payment* to *your* PayID and *you* will need to provide them with *your* BSB and Account number.

## **8. Maintaining PayID Details**

*You* must keep *your* PayID details current, accurate and complete and cancel *your* PayID immediately in circumstances where *you* no longer own or have authority to use *your* PayID.

## **9. Locking Your PayID**

- 9.1 *You* are able to temporarily stop *payments* being made to *your* PayID by locking *your* PayID via online or mobile banking.
- 9.2 While *your* PayID is locked, *payments* received by *us* addressed to *your* PayID will be rejected by *us*, returned to sender and not credited to *your* *linked account*.
- 9.3 We may lock *your* PayID at any time without notice to *you* if we reasonably suspect that *your* PayID has been used for fraudulent or illegal purposes.
- 9.4 *You* will not be able to transfer *your* PayID while *your* PayID is locked.

## **10. Transferring Your PayID to a Different Account**

- 10.1 *You* are able to request transfer of *your* PayID to another *account* *you* hold with *us*, or to an *account* *you* hold with another financial institution.
- 10.2 Transfer of *your* PayID to another *account* *you* hold with *us* generally takes effect immediately, but there is no guarantee that this process will be done immediately.
- 10.3 If *you* transfer *your* PayID to an *account* *you* hold with another financial institution, *you* must follow the PayID creation procedures of that other financial institution.

10.4 Until such time as the transfer of *your* PayID to another eligible *account* is completed, any *payment* made to *your* PayID will continue to be directed to the current *linked account* you hold with *us*.

## **11. Closing Your PayID**

11.1 *You* are able to close *your* PayID at any time.

11.2 *We* may close *your* PayID where:

- (a) *we* are not satisfied that *you* own or are otherwise authorised to use that PayID;
- (b) *we* reasonably suspect that the PayID is or has been used for a fraudulent or illegal purpose;
- (c) *your* PayID has remained locked for a period that *we* reasonably consider to be excessive; or
- (d) *we* are required to do so by law or by the operator of the NPP.

11.3 *We* will automatically close *your* PayID if the *linked account* to which that PayID is attached is closed.

11.4 When *your* PayID *linked account* is closed with *us*, *your* PayID is removed from the *PayID service* that *we* maintain

## **12. Liability**

12.1 The provisions of Part 4, Section 1 (*Payment Facilities and Services Electronic Banking*) of this DPS apply to *payments* made to a PayID to the extent that they are not inconsistent with these *PayID terms*.

12.2 The provisions of this DPS dealing with *mistaken internet payments* apply to *payments* sent to the PayID of another person.

12.3 The provisions of this DPS dealing with *mistaken internet deposits* apply to *payments* made by another person to *your* PayID.

## **13. Privacy and Disclosure**

13.1 To enable *you* to use a PayID *we* will need to record *your* PayID, *PayID name* and *account* details and other personal information with the *PayID service* or its service providers.

13.1 If *we* do not disclose *your* personal information to the *PayID service* or its service providers *we* will not be able to provide the *PayID service* to *you*.

- 13.2 Where *your linked account* is a *joint account*, other *account* holders may be able to see messages and notifications associated with *payments* and other messages addressed to *your* PayID.
- 13.1 You agree to us disclosing to the *PayID service* and its service providers (and in the case of a *joint account* the other *account* holders) such of *your* personal information as is necessary in order for us to facilitate the provision of the *PayID service* to you.

#### 14. Definitions

For the purposes of these *PayID terms*, the following definitions apply:

**Linked account** – any *account* where you have associated a PayID with and linked a PayID to that *account*.

**Payee** – means a person to whom you make an Osko *payment*.

**PayID** – means any of the following, which can be linked to an *account*:

- (a) mobile telephone number or email address;
- (b) for business customers, ABN, ACN, ARBN or ARSN; or
- (c) any other type of identifier as permitted by the NPP and supported by us.

**PayID name** – means the name registered with a PayID, intended to help identify the recipient of the PayID in the *PayID service*. It must reasonably reflect *your* real name.

**PayID service** – the registry created under the NPP where PayIDs are recorded and administered.

**PayID terms** – the terms contained in this section of the DPS.

This page has been intentionally left blank



This page has been intentionally left blank

This page has been intentionally left blank

This page has been intentionally left blank

## WE'RE HERE TO HELP

It's easy and convenient to contact us.

Here's how:



**1800 033 139** (8am to 8pm AEST weekdays)



**visit your local Defence Bank branch**



**defencebank.com.au**



**info@defencebank.com.au**



**Video call app**

### **Defence Bank Limited**

ABN 57 087 651 385 AFSL/Australian Credit Licence 234582

Head Office, Level 5, 31 Queen Street

Melbourne VIC 3000

B025 (02/18)



**Defence Bank**