Defence Bank

defencebank.com.au
1800 033 139

# Supplementary Defence Bank Products and Services Conditions of Use.

Effective 15 April 2025.

This Supplementary Defence Bank Products and Services (SDPS) Conditions of Use outlines the changes to the Defence Bank Product and Services Conditions of Use, dated 1 November 2024 a result of changes to Defence Bank's product & services terms and conditions.

In this document where we refer to the expression "DPS" we are referring to the Defence Bank Products and Services Conditions of Use – Version effective from 15 April 2025.

The information contained within this SDPS must also be read in conjunction with the DPS dated 1 November 2024. If you require a copy of the DPS, you may obtain this from our website or by contacting one of our branches or our Contact Centre on 1800 033 139.

**The purpose of this SDPS is to highlight the changes (see below) to our term deposit grace period and how you can provide us instructions as it relates to your term deposit maturity as at 10 April 2025. Refer to page 8 & 9 of the DPS dated 1 November 2024 for more details.**

**Section 3.8.1 Reinvestment/Redemption.**

**From:**

You should let us know what you would like to do either before the maturity date or up to five business days after the maturity (the Grace Period – see below).

**To:**

You should let us know what you would like to do either before the maturity date or up to seven calendar days after the maturity (the Grace Period – see below).

**Section 3.8.2 Grace Period.**

**From:**

A grace period of five business days from the date of investment is provided, for new or re-invested term deposits during which you may withdraw or transfer funds without penalty, subject to minimum investment amount. No interest is payable on withdrawn amounts during the grace period.

**To:**

A grace period of seven calendar days from the date of investment is provided, for new or re-invested term deposits during which you may withdraw or transfer funds without penalty, subject to minimum investment amount.

Defence Bank

defencebank.com.au
1800 033 139

# Supplementary Defence Bank Products and Services Conditions of Use.

Effective 15 April 2025.

**We have added new wording to section 3.8.2 under Grace Period:**

Where you add funds during the seven calendar days 'grace period', interest will accrue on the additional funds from the date the additional funds are deposited into the Term Deposit account.

Where you withdraw funds during the seven calendar day 'grace period', interest will accrue on the remaining daily balance (less the amount withdrawn) at the prevailing interest rate.

**We have also added new section called Home Loan Offsets to our DPS of which includes:**

**Home Loan Offsets.**

A Home Loan Offset Account can only be linked if the account holder and borrower are the same person or persons. No interest will accrue to your account even when the balance falls below the required minimum balance, or the loan is repaid.

Our acceptance of your application to open a Home Loan Offset Account operates as a variation of the method of calculation of interest under your home loan contract as follows:

(a) when calculating interest on your home loan, the outstanding balance of the loan account balance used for the calculation of interest will be reduced by the Home Loan Offset Balance

(b) we calculate the Offset Balance by multiplying the balance of your Home Loan Offset Account, at the end of the day, by the offset rate.

The offset rate is 100%.

# We're here to help.

It's easy and convenient to contact us.

**Here's how:**

- 1800 033 139
- visit your local Defence Bank branch
- defencebank.com.au
- info@defencebank.com.au

Defence Bank

defencebank.com.au
1800 033 139

# Products and Services.

# Conditions of Use (DPS).

Effective 1 November 2024.

Defence Bank Limited ABN 57 087 651 385 AFSL/Australian Credit Licence 234582.
Head Office, Level 10, 31 Queen Street, Melbourne VIC 3000.

# Table of contents

## 1. Welcome!

Thank you for considering Defence Bank. By joining us you'll become a member of a mutual bank that exists to serve its members, not shareholders. Our Purpose is to serve those who protect us, reinvesting all profits back into banking products and services that are tailored to meet the needs of ADF families, while also remaining competitive for all Australians who support the Defence community.

### 1.1. What this document covers.

This document, the bank's Products and Services Conditions of Use (DPS), contains important information and terms and conditions about the deposit products and payment facilities we offer.

This document covers our account facilities, how to access and use them, account management, cheques and our electronic banking products, namely Online Banking, Mobile Banking, BPAY, Pay ID, OSKO and PayTo. It also covers your rights and obligations with us.

Some words used in this document have special meanings, to make it easier to read, take some time to go through the "definitions".

### 1.2. How these terms and conditions become binding on you.

As soon as you open an account or use an access facility you become bound by these terms and conditions.

Where you authorise another person to operate on your account, you must give that other person a copy of these terms and conditions and ensure that the authorised person complies with them.

Other terms and conditions, including those implied by law, also apply, but these terms and conditions prevail in the event of any inconsistency to the extent permitted by law. If the law implies terms and conditions which cannot be excluded, our liability under those implied terms and conditions will be limited to the maximum extent permitted by law.

## 2. Our accounts and payment facilities.

We offer a range of savings and transactional accounts and payments facilities.

Details can be found in the **Summary of Accounts and Access Facilities** document. You can find this document on our website or we can send you a copy on request.

## 3. Information about our accounts.

### 3.1. Am I eligible to open an account?

The Bank services are available to all serving Defence personnel of Australia and its allies, veterans and all other Australian's (both citizens and/or residents) with an affinity to the Defence Force to support and strengthen the Bank's bond.

As long as you're an Australian resident for taxation purposes, have an Australian residential address and you have provided Defence Bank with all of the information we require to determine your Foreign Tax Residency Status; then you can open an account with us.

Alternatively, if you are an international visitor, you can contact us to discuss your options.

The Defence Bank board has discretion when it comes to determining other appropriate membership categories.

### 3.2. How to open an account.

From 8 July 2024 if you are new member to the bank and you are an individual, or sole trader over the age of 18 years, we will provide you with an everyday access account to get you started.

If you require an additional account, you can open an account:

- online at defencebank.com.au
- in person at any branch; or
- contact us over the phone on **1800 033 139** for an application.

If you're an existing member or customer you can open an account:

- in online banking at defencebank.com.au
- via the Defence Bank App.
- in person at any branch; or
- contact us over the phone on **1800 033 139** for an application.

There are specific terms and conditions for opening an account. Please first check the Summary of Accounts and Access Facilities document for the different account types available, any special conditions for opening, and the features and benefits of each account type.

### 3.3. Account signatories.

At any time you can authorise us to allow another person to operate on your accounts ('authorised person').

To appoint an authorised person you and the person you are authorising, will need to complete and sign a request form. You can allow an authorised person to operate some or all of your accounts.

You are responsible for all transactions your authorised person carries out on your account. You should ensure that the person you authorise to operate your account is a person you trust fully.

You may revoke the authorised person's authority at any time by giving us written notice.

We may limit or restrict the ability of another person to operate on your account in our sole and absolute discretion.

By giving access to an authorised person you are giving them authority to some, or all of the following:

- Transfer money/pay someone.
- Access Online Banking and the App facilities.
- Make a Bpay payment.
- Make international transfers.
- View balances and transaction history.
- Set up notifications (alerts).
- Set up Pay ID.
- Make cash withdrawals.
- Remove themselves as a signatory.
- Update their own details.
- Signatory authority in relation to PayTo Payment Agreements.

For all other transactional activities/requests must be completed by the account owner.

Each account holder and person authorised by an account holder, discharges and indemnifies us from and against all actions, proceedings, accounts, claims, demands, losses and damages, including any costs that we reasonably incur, arising from or in any way relating to us in good faith:

- acting on instructions. received by mail or electronic means (whether by facsimile, telephone, internet, ATM, or EFTPOS), which we have reasonably determined, given or signed by the account holder, the adviser, an authorised representative or an authorised third party signatory or, in the case of a joint account holder, by any of them; and
- releasing information about you or the account to anyone that we have reasonably determined is authorised to receive that information (including and authorised representative or third party signatory appointed by the account holder).

### 3.4. Proof of identity.

We will verify your identity and the identity of any authorised person on your account in certain circumstances, including:

- when you become a member or first open an account.
- when you are added as an authorised person to an account, and
- periodically during our relationship with you.

We do this by collecting information about you, such as your name, address and date of birth and then verifying that information against your identity documents, such as a current driver licence or passport.

### 3.5. Tax file number (TFN).

Government legislation states that all accounts earning deposit interest in a tax year may be subject to Tax File Number (TFN) legislation. We will ask you for your Tax File Number or exemption. If you are a businesses we will ask for your ABN instead of your TFN. For a joint account, each joint holder must quote their TFN and/or exemptions.

You do not have to disclose your TFN or ABN but if you do not, we may deduct withholding tax from interest paid on the account at the highest marginal tax rate (plus the Medicare levy). If you provide us with a residential address outside of Australia your account/s will be subject to non-resident withholding tax.

### 3.6. Joint accounts.

Some accounts may be opened jointly with your partner, family members or a group of people.

The credit balance of a joint account is held jointly by all account holders. This means that each account holder has the right to withdraw all available funds (including up to the limit of any available credit facility) in the account.

Joint account holders must all sign an authority telling us how the account is to be operated. The authorised 'method of operation' can be:

- jointly – where two or more account holders must act together; or
- separately – where account holders may act individually.

Where you have selected the 'method of operation' as either jointly or separately, you have the option to change these around at later date by contacting us. If you no longer require a joint account, the joint account must be closed and a new account opened in the individual's name. We require a written authority from all account holders to do so.

Also, regardless of any authorities to operate, any party to a joint account can require us to

- operate the account only on the signature of all parties;
- suspend the account to allow the joint account holders time to reach agreement about dispersal of the account funds, in which case these instructions will remain in effect until all joint account holders agree otherwise. This might be done if there is a dispute between the joint account holders. Visit any branch or call us for assistance. If you ask for an account to be operated jointly, some account features may not be available (for example, card access).

It's important to understand your responsibilities prior to opening a joint account.

You should know that:

- to open a joint accounts, all account holders must be identified.
- the liability of joint account holders on an account is joint and several so if one or more account holders overdraws the account, each joint account holder will be liable for payment of all or any part of the amount overdrawn.
- you can view the accounts you have with joint account holders in Online Banking. All joint account holders can authorise to share access to the account with your other authorised users in Online Banking.
- we may accept a cheque into a joint account which is payable to any one or more named account holders.
- if one joint account holder dies any credit balance in the joint account will belong to the surviving account holder(s).

### 3.7. Trust account.

Trust accounts can be opened on request.

One or more persons may open an account in which they are named as trustee for another person(s). For example, a trustee account held by:

- parents for children.
- trustees under a will.
- trustees for clubs and other organisations.
- trustees of a self-managed superannuation fund.

When you open a trust account we will ask you for a copy of the trust deed. We may ask you for further information to verify your identity, the status of the trust and the identity of the beneficiaries of the trust.

You represent and warrant each time you transact on a trust account that you are acting in accordance with the terms of the trust and that the transaction is authorised under the terms of the trust.

Each time you transact on the trust account we are entitled to rely upon your representation and warranty and are not required to verify or make any enquiries in relation to your operation of the account or determine whether a transactions on the account is authorised by the terms of the trust.

Each trustee of a Trust is an owner of the account.

If any of the trustees change, you need to let us know straight away. The trustees are responsible for the account and ensuring that the Trust complies with relevant laws.

### 3.8. Term deposits.

Term deposits are a simple form of investment. You can put money into a term deposit for the time that you choose (the term) and receive a fixed rate of interest for that time. There are minimum and maximum amounts that apply to term deposits – Refer to our website and Interest Rate Schedule for details.

When you setup a term deposit we will send you a Certificate of Investment which details the deposit amount, interest rate and term.

The interest rate is fixed at the time of the initial deposit and for the full term. Interest is calculated and accrues daily. For more details on our interest rates, refer to our Interest Rate Schedule and Summary of Accounts and Access Facility document located defencebank.com.au or by calling us.

Where the term does not exceed 12 months, interest that has accrued on the deposit is paid on the date of maturity. Where the term exceeds 12 months, interest that has accrued on the term deposit during a year is credited to the term deposit account at the end of each year and on maturity.

We may offer special rate term deposits from time to time, known as 'Premium Certificate term deposits', which may have their own specific terms and conditions. Please check our latest term deposit information on our website.

While a term deposit is intended to be held for the agreed term (until maturity), you can access your money any time upon request but a pre-payment adjustment and a fee may apply as detailed in the Defence Bank Fees and Charges Schedule.

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.

#### 3.8.1. Reinvestment/Redemption.

When your term deposit approaches maturity we will contact to you letting you know the maturity date and the reinvestment options available and ask whether you would like to redeem or reinvest it.

To provide us with redemption instructions prior to your maturity date you have two choices, you can complete a form or lodge your request in on-line banking.

You should let us know what you would like to do either before the maturity date or up to five business days after the maturity (the Grace Period – see below).

If you wish to redeem or vary the terms of the term deposit, your request will be actioned on the maturity date, the next business day, or before the end of the Grace Period.

If we don't receive instructions from you by the end of the Grace Period, then your term deposit and interest earned will be reinvested for the same term at our advertised interest rate applicable on the date of maturity. The interest rate on the reinvested term deposit may be lower than your initial term deposit. Where we are unable to contact on two or more occasions relating to your term deposit, we may close your term deposit and pay the proceeds to another of our deposit product accounts.

If the same term isn't available then your term deposit will be reinvested at the closest standard term (i.e. not a special offer, premium certificate term) to the original term. Any requests for variations to the terms of your term deposit received after the grace period has ended, may incur a pre-payment adjustment and a fee may apply.

### 3.8.2. Grace period.

A grace period of five business days from the date of investment is provided, for new or re-invested term deposits during which you may withdraw or transfer funds without penalty, subject to minimum investment amount. No interest is payable on withdrawn amounts during the grace period.

### 3.8.3. Early Redemption of Your Term Deposit.

The Term Deposit is intended to be held for the agreed term, until maturity. Despite this, you can access your Term Deposit amount before maturity.

A pre-payment adjustment and a fee will 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 Defence Bank Fees and Charges Schedule.

### 3.8.4. 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 an early redemption fee will apply.

| Percentage of the term lapsed. | Adjustment to be applied as a % of your interest rate. |
|---|---|
| 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% |

Prepayment adjustment example: For a 5.00% p.a. one-year term deposit of $50,000, where the entire account balance was withdrawn after 4 months:

1. Divide the original interest rate by 365 to get the daily interest rate 5.00% ÷ 365 = 0.0136986%
2. Multiply this by the amount of the term deposit to get the interest earned each day $50,000 x 0.0136986% = $6.8493
3. Multiply this by the number of days for which the funds were deposited $6.8493 x 122 days = $835.62
4. Find the percentage of the original term that has elapsed 122/365 (days) = 0.33 (33%). As 33% of the original term has passed, the interest will be reduced by 80%.
5. Multiply the interest earned by 80% (0.80) to get the prepayment interest reduction $835.62 x 0.80 (80%) = 80% $668.49 (rounded to two decimal places). This is the interest you will lose if you close your term deposit early. These calculations do not include the early withdrawal fee, see the Defence Bank Fees and Charges Schedule for more details.

Note that the calculation above is intended as a guide only, and may vary slightly from your actual interest earned due to the rounding used in the example.

### 3.8.5. Business term deposits.

Business term deposits are available to Sole Traders, Corporates (including Corporate Trustees), Individual Trustees, Partnerships, Incorporated Associations (not-for-profit organisations and clubs) and operate in the same way as term deposits do.

### 3.9. Salute account.

The Salute account is a high interest savings account that rewards Australian Defence Force (ADF) members who have met one or more ADF milestones. We want to salute and reward those members who achieve the important milestones with the ADF. Where you notify us within 12 months of reaching one of the following milestones you will then be entitled to open a Salute account and we will pay you a bonus fixed rate of interest on monies deposited in the Salute account for a promotional period (currently 12 months) provided you make minimum deposits to an Everyday Access account each month (current minimum is $1,500.00 per month). The bonus fixed rate begins when you first open your account.

The milestones are:

1. You have reached 15 years of service in the ADF.

2. You have reached 25 years of service in the ADF.

3. You are deployed.

4. You start receiving a seagoing allowance.

5. You retire from the ADF.

6. You resign from the ADF, or;

7. You are discharged from the ADF on medical grounds.

Each time you first reach a milestone you may open a new Salute account. i.e. you may only open one new account per milestone.

A Salute account may be held either solely in the name of the member who has reached a milestone, or can be held in jointly with another.

If, during the 'promotional period', you no longer meet the condition of a minimum $1,500 per month deposit to your Everyday Access account, we will contact to you requesting that you do so. If, at the end of the 30 day period you have not met the condition, then at Defence Bank's discretion we may treat your Defence Bank Salute account as a Defence Bank Everyday Access account and the Salute bonus and bonus interest rate will no longer be applied.

For details of the tiers and maximum promotional current interest rates payable both during and after the promotional period, please refer to the Interest Rate Schedule or go to our website. The Salute Account is available on deposits up to $1 million.

## 4. Operating your account.

### 4.1. Putting money in.

Deposits to an account may be made:

- by cash or cheque at any branch.
- by direct credit, e.g. from your employer for wages or salary.
- by transfer from another account held either with Defence Bank or with another financial institution.
- at Australia Post via Bank@Post™
- by mail (cash not permitted).

Further information about our various access and payment facilities are set out later in this document.

Please check our Summary of Accounts and Access Facilities document for details as to which deposit options are available for your account type; and read the Defence Bank Fees and Charges Schedule for more information.

### 4.2. Taking money out.

Unless otherwise indicated in our Summary of Accounts and Access Facilities document, withdrawals from an account may be made:

- over the counter at any branch or at Australia Post via Bank@Post™.
- via internet banking (including mobile and digital wallet).
- via BPAY.
- at ATMs, using a linked VISA Debit card, or by Visa Credit card (fees may apply)
- via EFTPOS terminals, using a linked VISA Debit card.
- by international telegraphic transfer.
- by Direct Debit.
- by Auto Transfer.
- via PayTo.

Further information about our various access and payment facilities are set out later in this document.

Please check our Summary of Accounts and Access Facilities document for details as to which withdrawal options are available for your account type, and read the Defence Bank Fees and Charges Schedule.

### 4.3. Deposit and withdrawal conditions.

We may limit the amount of payments or transfer you may make on any one day. We will advise you of the applicable transaction limits.

Cash withdrawals made in branches are limited to $5,000 per day, per member, if you require more than this limit you will need to provide us with at least 1 business days' notice.

In processing deposits to your account, we will rely on the account number only. We do not check any account name specified on the deposit instructions. The funds will be deposited into the account number specified on the deposit instructions.

Proceeds of any cheque deposited in your account will usually not be available until the cheque is cleared. If you need a cheque cleared faster than that, you can ask for 'special clearance'. If we make the proceeds of a cheque available prior to the cheque being cleared and the cheque subsequently fails to clear, we will debit the corresponding amount from your account.

We may refuse to process a withdrawal from your account if your account has insufficient credit funds (including available credit limit if your account has an agreed overdraft facility) available to satisfy the withdrawal.

We are responsible for a deposit into a facility received by our electronic equipment, from the time you complete the deposit, subject to verification of the amount deposited. If there is a discrepancy between the amount specified as being deposited and the amount actually received by us, we will contact you as soon as practicable about the difference. Electronic deposits may not be processed on day of receipt.

There is no minimum account balance required on our transactional and savings accounts.

### 4.4. What interest can I earn on my account?

We pay interest on some accounts. Please refer to our website and Interest Rate Schedule for more details.

Our Summary of Accounts and Access Facilities document explains how we calculate and credit interest to your account.

We may vary interest rates from time to time, except for term deposits where interest is fixed for the term.

### 4.5. What happens if I change my contact details?

If you change your name, address, phone number or email address, please let us know as soon as possible so that we can continue to contact you. Contact details can be updated in both the App and in Online Banking.

If you do not update your contact details any correspondence sent to your old address or email address is still considered 'notice in writing'. We will also not be responsible for any errors or losses associated with changes to your details where we have not been notified of the change.

### 4.6. What happens if I change my name?

If you change your name you need to let us know. To do this you can bring your identification documents to our branch or alternatively you can contact us and discuss your options.

### 4.7. Account statements and notices.

#### 4.7.1. Sending you statements.

By opening a new membership online you agree to receive your bank statements electronically along with other communications. We will send you notification when a new eStatement or other communication becomes available to view.

Generally, all your accounts will appear on a single statement and in certain circumstances when required, we will issue a statement separately.

For Joint accounts, Defence Bank can send statements of accounts, changes to the DPS and other notices by mailing or emailing them to the first named account holder at the mailing address or address we hold.

If you do not wish to receive your statements or other communications electronically you can opt out any time via the Mobile app, online banking or by calling us. We may charge a 'record search fee' for statements, for more information refer to the Defence Bank Fees and Charges Schedule.

#### 4.7.2. Frequency of issue of statements and other notifications.

For accounts with a line of credit or overdraft attached we will send you statements monthly.

For all other savings and transactional accounts we will send you statements of account half yearly, in January and July each year.

If you are registered for online banking you may view transactions and issued statements online at any time.

Other notices may be sent with eStatements or separately.

You can also ask us for a statement at any time, however we may charge a record search fee for providing additional statements or copies, see the Defence Bank Fees and Charges Schedule for more information.

PayTo notifications will be delivered either by our online banking and mobile app solution, or by email immediately.

#### 4.7.3. Statements - general matters.

We recommend you keep your email address up to date so we can send you notifications and we can contact you.

We also recommend you:

- Check your statements as soon as you receive them and immediately notify us of anything you think is incorrect.
- Check your online transaction history regularly to make sure it reflect your recent deposits, payments and purchases accurately and immediately notify us of anything you think is incorrect.
- Regularly check your emails for communication from us.

### 4.8. Spend Tracker.

'Spend Tracker' allows you to track cleared payments from eligible accounts (as detailed in the Summary of Accounts and Access Facilities document) in the Defence Bank app.

'Spend Tracker' is only an indicator of your spending and will not restrict your spending or saving from your Defence Bank accounts.

### 4.9. Overdrawing your account?

You must not overdraw your account without our prior agreement.

Your account can become overdrawn either when you have a negative balance, or where the account has exceeded your overdraft limit. Any amount overdrawn without our prior agreement is repayable immediately.

### 4.10. When can the bank transfer money between my accounts?

We can combine or set-off the balance of two or more of any type of accounts, credit facilities or other products held by you with Defence Bank, even if they are held in joint names. This may happen when an account is overdrawn or is in debit and another is in credit.

For example, the credit balance in one account can be used to repay the debit balance in another account. We will promptly inform you if we exercise this right and need not give you notice in advance.

Neither you nor any other accountholder has a right of combination or set-off unless we have otherwise agreed in writing.

### 4.11. Dormant accounts.

If no transactions are carried out on your transaction or savings accounts for a period of at least 12 months (other than transactions initiated by us, such as crediting interest or debiting of fees and charges) your account will become dormant.

You will not be able to transact on an account which has become dormant.

We will continue to pay the current interest rate applicable to the account, provided the membership isn't classified as a 'dormant membership' (see Dormant memberships 4.12).

You may reactivate the account by making a deposit to the account from an external source or contact us and we will reactivate your account for you.

### 4.12. Dormant Memberships.

Where all transaction or savings accounts held by you have been classified as dormant we may consider your membership with the bank to be dormant and, in line with the requirements of the bank's constitution, redeem your member share. Where this occurs you will no longer be able to received financial accommodation from the bank or vote at the AGM. Before we redeem your member share we will contact to you providing at least 28 days-notice, asking if you want to keep your membership open which you can do so by reactivating one or more of your dormant transaction or savings accounts. If you do not reply we will treat your membership as dormant and redeem your member share.

When dormancy occurs, your membership share and any transactional or savings accounts will be closed and any balance outstanding consolidated into one dormant savings account.

Once your membership becomes dormant, we may:

- charge a dormancy fee (see the Defence Bank Fees and Charges Schedule).
- stop paying interest.

You may reinstate your membership with the bank at any time, subject to the provision of information required by the bank at the time to establish new memberships and accounts and any funds held in the dormant transactional or savings account will be reinstated to a new account, as offered by the bank, at the date of your request.

Where you have one or more of the following account types, you are exempt from the dormancy (and unclaimed monies) processes:

- term deposits.
- loan accounts, including credit cards and overdrafts.
- children and teens account (17 yrs old or younger).

### 4.13. Unclaimed monies

If there is no activity on your membership the bank may be required to remit funds to ASIC in line with the currently applicable requirements of section 69 of the Banking Act in relation to unclaimed monies.

For more information visit asic.gov.au and search unclaimed money.

### 4.14. When we may close your account.

We may close your account at any time at our discretion and we will generally give you notice before closing your account. Where your account has a credit balance, before it is closed we will either take reasonable steps to return the balance to you or transfer the balance to the Commonwealth Government as unclaimed money where the relevant statutory requirements have been met for doing so.

If your account has a balance of $0 for 12 months or more we may close your account. In doing so we will provide you notice. .

### 4.15. Closing your account.

You can close your Defence Bank account and access facility at any time by contacting us.

We will ask, where relevant, that you return any VISA Debit card at that time. If you do not return your card to us, you will remain responsible for any further transactions which may happen where the merchant is not required to get authorisation.

We may defer closure and withhold sufficient funds to cover payment of uncleared cheques, electronic transactions and fees, if applicable.

You can also cancel any access facility on request at any time but leave the account open.

### 4.16. Suspension or termination of accounts and services.

We may suspend access to an account and services when:

- we identify your account is operating in a manner that we have reasonably determined that is either unsatisfactory or inconsistent with the terms and conditions.
- Defence Bank Products and Services must not be used for financial abuse, unlawful activities, or engaging in offensive, threatening, defamatory, harassing, or controlling behaviour. Where Defence Bank identifies any such behaviour this may result in access to services and / or accounts being either suspended or terminated.
- where we are unable to immediately validate a transaction without first contacting you.
- subject to certain circumstances we may notify you that we have taken this action.
- you close the last of your accounts with us.

You remain liable for any transactions carried out after the cancelation or termination date. If there are any refunds or other credit payments that occur prior to cancellation but are received by us after cancelation, we will credit these to you.

You should return or destroy any cancelled VISA Debit card.

### 4.17. Fees and charges.

Fees and Charges may be applicable to accounts and access facilities and if applicable are detailed in the Defence Bank Fees and Charges Schedule and also via our product pages on our website. All applicable fees and charges will be charged to the relevant account.

You may obtain a copy of the Defence Bank 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 or by calling 1800 033 139.

### 4.18. Merchant surcharge.

Some merchants and electronic terminals charge a surcharge for making electronic 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.

### 4.19. Government taxes and charges.

We will debit all applicable government taxes and charges to one or more of your accounts as we choose.

If there is a change to, or introduction of a government charge that you directly or indirectly pay as part of your banking service, we will tell you about this reasonably promptly after the government notifies us, unless the government itself publicises the introduction or change.

### 4.20. Using a BSB and account number.

You may make and receive payments using our BSB and your account number as an identifier.

Where you do so it is your responsibility to make sure that the BSB and account number used are both correct.

While you may specify the name of the account holder you acknowledge that neither us nor a receiving institution use the name of the account as an identifier and do not check that the BSB and account number used matches the name of the account holder.

Where you use an incorrect BSB and/or account number and the payment is misdirected you or the person making the payment to you may be able to claim back monies mistakenly paid as a mistaken internet payment in the circumstances outlined in this document.

## 4.21. Using a PayID.

### 4.21.1. What is a PayID.

A PayID is a smart address used to receive payments to your account through the New Payments Platform (NPP) instead of using your account number and BSB to identify the account to which payment is to be made. A PayID is a bit like a nickname for your account.

You can create multiple PayIDs but a PayID can only be linked to one account at a time.

You do not need to create a PayID. Creation of a PayID is optional. You can continue to operate your account without a PayID, in which case payments to your account will require your BSB and account number.

### 4.21.2. How to create a PayID for your account.

You create a PaylD by linking an eligible account to a PaylD you create. Your PaylD must be associated with a name (your PaylD Name) which reasonably represents you, such as your mobile number, email address or your ABN (if applicable.) We need to approve your chosen PayID.

### 4.21.3. Using your PayID on your account.

A PaylD, once linked to your account, can be used by others to make NPP payments to you through the New Payments Platform without them having to enter your account number and BSB, provided they are permitted to do so by their financial institution.

Once a PayID is linked to your account, you simply provide your PayID to others so they can make payments to you instead of handing out your BSB and account number.

You can create a PayID for an eligible account through Online Banking.

### 4.21.4. PayID conditions applicable to creating and using a PayID on your account.

By creating a PaylD, you agree that your PaylD name may be shown to anyone who looks up your PaylD (for example, to make a payment to you).

In establishing a PayID, you represent and warrant that:

- you own, or are authorised to use the PayID you have created.
- the PayID is current, accurate and complete; and
- you agree to your PayID being registered in the PayID service.

Before you can use a PayID you must first satisfy us that you own or are authorised to use your chosen PayID. We may ask you to provide evidence to establish this to our satisfaction. We may reject your use of any PayID where in our opinion you are not the owner or authorised to use that PayID. We can also refuse your request to create a PayID where:

- we have yet completed verifying your identity.
- we reasonably suspect that the PayID is or has been or will be used for a fraudulent purpose.
- we are required to do so by law or by the New Payments Platform operator; or
- the PayID is already in existence.

Where your attempt to create a PayID fails because that PayID is already created by someone else in the PayID service, we will try to assist to resolve this by contacting the financial institution or other entity that registered that PayID, who is then required to contact the customer to which the PayID is registered to establish if that customer has the right to use the PayID. If that person cannot establish that they are the rightful owner of the PayID, their financial institution is required close that PayID.

You must promptly notify us of any change in your personal details including if you cease to own or cease to be authorised to use your PayID or your linked account. You may notify us by calling 1800 033 139.

Where your account is held in joint names, each account holder can link a PayID to the account. Additionally, each authorised signatory on the account may establish a PayID on the account.

You may choose to create more than one PayID for your account provided each PayID is unique.

Once a PayID is created and linked to your account, you may not use the same PayID in relation to any other account with us or with any other financial institution.

We may restrict some PayID Names or PayID types if they are:

- identical to another PayID in the service.
- restricted for use only by business customers and organisational payers.
- likely to mislead or deceive a payer into sending you payments intended for another payee or for any other reason which, in our reasonable opinion, is inappropriate.
- if the PayID created is considered by us or the PayID Service to be offensive or otherwise undesirable.

Depending on the payer's financial institution, your PayID Name may be displayed to payers who send payments to you.

At the same time you create your PayID Name, we will either enable you to:

- confirm your selection of a PayID Name for display to payers; or
- select an alternative PayID Name, such as your business name, for display.

We will not permit a PayID Name we consider could reasonably mislead or deceive a payer into sending you a NPP payment intended for another payee.

You must keep your PayID details current, accurate and complete.

You must notify us immediately if you no longer own or have authority to use your PayID.

**4.21.5. Transferring your PayID to another account.**

You can request a transfer of your PayID at any time from one account to another. However, a locked PayID cannot be transferred.

You can generally transfer your PayID to another account (including an account with another financial institution).

To transfer your PayID to another account you must submit a request to us. A request can be submitted online through our internet banking site, via or our mobile app or by visiting a branch or by telephone.

We will endeavor to complete a request to transfer or close a PaylD within 24 hours.

If you are transferring a PaylD to another institution, you will also need to request that institution to link the PaylD to your account with that institution and they may take longer to process the request. The other financial institution may also require you to take steps to complete the transfer.

Once the PaylD is linked to your new account, payments made to the PaylD will be directed to that account. Until the transfer is effected, all payments to your PayID will continue to be directed to your current linked account.

If the new financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain attached to your linked account with us. This means NPP Payments to your PayID will continue to be directed to your account with us. You can request to transfer your PayID again at any time.

Note: Transferring a PayID [to another financial institution] will cause payments under any PayTo Payment Agreement linked to that PayID to fail unless you also transfer the Payment Agreement: see Sections 16.7.20 & 16.7.21.

**4.21.6. Transferring your PayID from another account.**

You can transfer a PayID that you have created for an account with another financial institution to an eligible account with us by initiating the transfer process with the other financial institution and notifying us once this has been done so that we can complete the transfer process.

Note: If the PayID is linked to a PayTo Payment Agreement, the Payment Agreement will not automatically transfer with the PayID. You will need to take additional steps if you wish to transfer the Payment Agreement to your account with us: see Section 16.4.4.

#### 4.21.7. Locking your PayID.

We monitor PayID use to manage misuse and fraud.

You acknowledge that we have the right to and agree to us locking your PayID if we reasonably suspect misuse of your PayID or where your PayID has been used to procure payments fraudulently.

A PayID may not be used to receive NPP Payments, be transferred or updated while locked.

You will need to contact us to unlock a locked PayID

#### 4.21.8. Closing your PayID.

You can submit a request to close your PayID by submitting a request to us online (via our internet banking site or our mobile app), by visiting a branch or over the phone by calling.

We can close your PayID where:

- we are not satisfied that you own or are otherwise authorised to use that PayID.
- we reasonably suspect that the PayID is or has been used for a fraudulent purpose.
- your PayID has remained locked for a period that we reasonably consider to be excessive; or
- we are required to do so by law or by the operator of the New Payments Platform.

We will automatically close your PayID if the linked account for that PayID is closed.

Note: Closing a PayID will cause payments under any PayTo Payment Agreement linked to that PayID to fail unless you also transfer the Payment Agreement: see Sections 16.7.20 & 16.7.21.

#### 4.21.9. Privacy and PayID.

By creating your PayID you acknowledge that you consent and authorise:

- us to record your PayID, PayID Name and account details (including full legal account name) (PayID Record) with the PayID Service.
- other NPP Participants to use your PayID information for the purposes of sending payment messages, enabling payers to make payments to you, and disclose your PayID Name for payment validation.
- us in order to provide you PayID to disclose your personal information to BPAY, its service providers and other participants involved in the New Payments Platform.

Your consent and authorisation operates as your express consent to store, use and disclose the your personal information (PayID information) to third parties including NPPA for the purposes of the registration in PayID and other NPP Participants for the purposes of enabling NPP Payments to be sent and received and for reasonable secondary purposes (such as tracing and investigations).

If we are unable to disclose your personal information to participants in the New Payments Platform and their service providers, we will be unable to provide you with services.

You must notify us of any changes to your relevant personal information that may be contained in a PayID Record.

## 5. Transacting on your account - in person.

### 5.1. At branches/outlets.

Depending on your account type you are able to transact on your account in person at:

- any of our branches.
- Bank@Post outlets.

### 5.2. Transacting at Defence Bank branches.

When transacting on an eligible account at a Defence Bank branch you must first register your signature with us by completing an account signing authority if you wish to use a signature to authorise a transaction on your account.

Cash withdrawals made in branches are limited to $5,000 per day, per member, if you require more than this limit you will need to provide us with at least 1 business days' notice.

### 5.3. Transacting at Bank@Post outlets.

You may transact on your accounts at Australia Post outlets displaying the Bank@Post logo by using a Visa Debit card linked to your eligible account.

## 6. Transacting on your account - direct debits.

### 6.1. ePayments Code applies to direct debits.

Direct debits are an electronic payment facility and the ePayments Code applies when you transact on your account via direct debit.

### 6.2. Authorising a biller to debit my funds.

You can authorise a participating biller to debit amounts from your account, as and when you owe amounts to the biller. The biller will provide you with a direct debit request for you to complete and sign to provide them with this authority.

We are not advised by the biller when a direct debit request is established or discontinued.

Acting on the authority of the biller's financial institution, we will debit your nominated account and transfer funds in accordance with instruction received from the biller's financial institution.

Where its established its not at the fault of the bank, we accept no responsibility for when the instruction is received from the biller's financial institution or on the date of which the debit is processed to the nominated account.

Any instruction received for payment on a non- business day will be processed and payment made on the next business day.

### 6.3. How do I cancel my direct debits?

Should you wish to cancel a direct debit please let us know. We will take action to cancel a direct debit facility linked to your transaction account within 1 business day if you ask us to do so. We will not tell you to try to cancel the facility with the biller or other direct debit user first (but we may suggest that you also contact the direct debit user and explain the benefits of doing this). This might prevent the debit(s) being processed and the payment to stop.

If you believe a direct debit initiated by a biller is in error, you should contact the biller to resolve the issue. Alternatively, you may contact us. If you give us the information we require we will forward your claim to the biller. However, we are not responsible for nor liable to compensate you for your biller's error.

### 6.4. When can the bank cancel my direct debits?

Your direct debit may be rejected if the account information you provide is incorrect.

We can cancel or suspend your direct debit facility if:

- consecutive direct debit instructions are dishonoured.
- we suspect any direct debit payments may be fraudulent.
- we suspect your account has been compromised or is at risk of being compromised.
- your account is overdrawn.
- you are in default of the terms and conditions of your account.
- we are required to by law.
- you or a joint account holder dies; or
- your account becomes dormant.

If we do this, billers will not be able to initiate a direct debit from your account under their direct debit request. Under the terms of their direct debit request, the biller may charge you a fee for each dishonour of their direct debit request.

If you tell us you wish to cancel only one of multiple payment arrangements associated with a single direct debit, we will advise you to establish a new facility for the payment arrangements you wish to maintain.

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, Home Loan Offset, iSaver, Salute, Max eSaver, 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.

Where there is a complaint, we will accept and process your complaint that a direct debit was not authorised or is otherwise irregular.

## 7. Transacting on your account - auto transfer.

### 7.1. ePayments applies to auto transfers.

Auto transfers are an electronic payment facility and the ePayments Code applies when you make an auto transfer.

### 7.2. Auto transfer.

You can set up an automatic transfer authority on an account so that specific amounts of money are regularly transferred to another account nominated by you provided there are sufficient funds in your account at the time we process the auto transfer.

The other account could be yours, for example, your mortgage account or credit card account; or it could be someone else's account, for example, family or someone you're paying regularly for a service.

It is your responsibility to ensure that there are sufficient funds in your account at the time we process the auto transfer. If there are insufficient funds available, we may not be able to make the transfer.

You can setup, change or cancel an auto transfer at any time through internet banking (including phone apps), by calling us or by visiting a branch.

Auto transfers are similar to direct debit but differ in that you can control the frequency and the amount, and you can stop the auto transfer at any time by notice to us.

You should maintain a record of any auto transfer that you have set up on your account.

We will endeavour to process an auto transfer in accordance with your instructions. Where its established its not at the fault of the bank, we accept no responsibility if any such transfer is not or cannot be made and accordingly will not incur liability through our refusal or ommission to make any or all of the payments instructed by your or arising from any late payment.

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.

Where three consecutive auto transfers fail your instructions will be removed you will need to re-establish your instructions by contacting us.

We may in our absolute discretion conclusively determine the order of priority of payment by us under any account.

## 8. Transacting on your account - direct credit.

A direct credit is an electronic deposit to your account. Direct credits are not a service provided by us, instead are a service provided by other financial institutions. Direct credits are not an electronic payment facility for the purposes of these terms and conditions except that the provisions dealing with 'mistaken internet payments' to your account apply.

You can arrange for a third party to electronically deposit (direct credit) funds to your Defence Bank account by providing our BSB number 833-205 and your account number, or your PayID if you have set one up (see section 4 on PayID).

We are not advised when a direct credit authority is established or discontinued by you with a third party.

Although the third party may provide us with the account name we will not use that in order to verify if the account details are correct. We rely solely on the account number/PayID to identify the account to be credited.

Where its established its not at the fault of the bank, 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.

If you provide incorrect information to the third party or the third party provides us with incorrect account information the direct credit may be rejected or paid into the wrong account.

We are not liable for any loss incurred as a result of rejected direct credits or funds credited in error to accounts due to incorrect account information being provided by a third party.

To change a direct credit you must contact the third party responsible for depositing funds to your account. We are unable to accept or action any request to cancel a direct credit facility or stop an individual direct credit.

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.

If you believe a direct credit has been incorrectly deposited to your account, you should notify us immediately.

## 9. Transacting on your account - BPAY.

### 9.1. ePayments Code applies to BPAY transactions.

The ePayments Code applies when you transact on your account via BPAY. However, the provisions of the Code dealing with Mistaken Internet Payments do not apply to payments made via BPAY.

### 9.2. Using BPAY.

You can use BPAY® to pay bills bearing the BPAY logo from those accounts that have the BPAY facility. When you tell us to make a BPAY payment you must tell us the biller's code number (found on your bill), your Customer Reference Number (e.g. your account number with the biller), the amount to be paid and the account from which the amount is to be paid.

We cannot carry out your BPAY instructions if you do not give us all the specified information, or if you give us inaccurate information.

### 9.3. Processing BPAY payments.

We aim to process your BPAY payments promptly, and you must tell us promptly if:

- you become aware of any delays or mistakes in processing your BPAY payment.
- you did not authorise a BPAY payment that has been made from your account; or
- you think that you have been fraudulently encouraged to make a BPAY payment.

Please keep a record of the BPAY receipt numbers on the relevant bills. A BPAY payment instruction is irrevocable.

Except for future-dated payments you cannot stop a BPAY payment once you have instructed us to make it and we cannot reverse it.

You should notify us immediately if you think that you have made a mistake in the details.

A BPAY payment is treated as received by the biller to whom it is directed:

- on the date you direct us to make it, if we receive your direction by the cut off time on a banking business day, that is, a day in Sydney or Melbourne when banks can effect settlements through the Reserve Bank of Australia; and
- otherwise, on the next banking business day after you direct us to make it. Please note that the BPAY payment may take longer to be credited to a biller if you tell us to make it on a Saturday, Sunday or a public holiday or if another participant in BPAY does not process a BPAY payment as soon as they receive its details.

Notwithstanding this, a delay may occur processing a BPAY payment if:

- there is a public or bank holiday on the day after you instruct us to make the BPAY payment.
- you tell us to make a BPAY payment on a day which is not a banking business day or after the cut off time on a banking business day; or
- a biller, or another financial institution participating in BPAY, does not comply with its BPAY® obligations.

If we are advised that your payment cannot be processed by a biller, we will:

- advise you of this.
- credit your account with the amount of the BPAY payment; and
- take all reasonable steps to assist you in making the BPAY payment as quickly as possible.

You must be careful to ensure you tell us the correct amount you wish to pay. If you make a BPAY payment and later discover that:

- the amount you paid was greater than the amount you needed to pay, you must contact the biller to obtain a refund of the excess; or
- the amount you paid was less than the amount you needed to pay, you can make another BPAY payment for the difference between the amount you actually paid and the amount you needed to pay.

Chargeback rights don't apply to BPAY payments – but if you notify us of a mistake, we'll do our best to recover the payment. If we can't do so within 20 days, you'll be liable for that amount.

### 9.4. Future-dated BPAY payments.

You may arrange BPAY payments up to 60 days in advance. If you use this option you should be aware of the following:

- you are responsible for maintaining sufficient cleared funds to cover all scheduled BPAY payments or, if the account is a credit facility, there must be sufficient available credit.
- if there are insufficient cleared funds or insufficient available credit, the BPAY payment will not be made.
- you are responsible for checking your account transaction details or account statement to ensure the scheduled payment is made correctly.
- you should contact us if there are any problems with your future-dated payment.
- you must contact us if you wish to cancel a future-dated payment before the date for payment. You cannot stop the BPAY payment on or after that date.
- If a future dated-dated payment cannot be processes due to insufficient cleared funds on two consecutive business days, on the three consecutive occasions, the auto transfer BPAY will be cancelled.

You can cancel a future-dated BPAY at any time before the payment is due. You should contact us if there is any problem with your future-dated payment.

## 10. Transacting on your account - using a Visa Debit card.

A Visa Debit card is an electronic payment facility and the ePayments Code applies when you transact on your account using a Visa Debit card.

When you transact on your account using a Visa Debit card additional terms and conditions apply to your linked account in addition to these terms and conditions. These additional terms and conditions are referred to as the Visa Debit card conditions of use.

The Visa Debit card conditions of use can be found on our website at defencebank.com.au

To the extent of any inconsistency between these terms and conditions and the debit card conditions of use, the Visa Debit card conditions of use prevail.

## 11. Transacting on your account - using a digital wallet.

A digital wallet is an electronic payment facility and the ePayments Code applies when you transact on your account using a digital wallet.

When you transact on your account using a digital wallet additional terms and conditions apply to your linked account in addition to these terms and conditions. These additional terms and conditions are referred to as the digital wallet terms.

The digital wallet terms can be found by searching for “digital wallet” on our website at defencebank.com.au

To the extent of any inconsistency between these terms and conditions and the digital wallet terms, the digital wallet terms prevail.

## 12. Transacting on your account - third party payment services.

### 12.1. Third party payment services.

There is a wide array of third party payment services available which you might use for online shopping or subscriptions, or possibly for receiving payments.

Each third-party payment service operates differently and comes with its own terms and conditions. You should familiarise yourself with the terms and conditions of any third party payment service you use as these will apply to any transactions made using those services. Defence Bank Conditions of Use do not apply.

If you have a dispute with, or mistaken payment through a third party payment service, you will need to deal directly with the service provider instead of us. The ePayments Code does not apply to us in relation to third party payment services, but may apply to the third party payment services provider.

## 13. Transacting on your account - international transactions.

### 13.1. How do I make and receive international transactions?

You can make international payments (also known as telegraphic transfer which are processed by Western Union Business Solutions Australia Trading as Convera) using internet banking or mobile banking. For more information regarding international transfers, refer to the Defence Bank International Money Transfer document at defencebank.com.au.

If you are travelling, you can use your Visa cards overseas at any EFTPOS or ATM facility but be aware that some overseas merchants and ATMs charge you for making a transaction.

You can pay for international online purchasing by using your Visa Debit card. For more information on Visa Debit card refer to our Visa Conditions of Use document.

### 13.2. Foreign currency conversion fee.

We will charge you with a foreign currency conversion fee (also known as foreign currency transaction fee) for each of the following types of transactions:

- transactions made overseas, to be converted into Australian dollars.
- transactions made in a foreign currency, to be converted into Australian dollars.
- 'card-not-present' transactions in Australian dollars with merchants located overseas.
- transactions in Australian dollars with financial institutions located overseas, or
- transactions in Australian dollars (or any other currency) that is processed by an entity outside Australia (together referred to as Overseas Transactions in Australian Dollars).

Please note that even though an online shopping website with a domain name that ends in '.com.au' might appear to be an Australian business, they or their bank might be located overseas. This means you could still be charged an international transaction fee.

For more information refer to the Defence Bank Fees and Charges Schedule.

## 14. Transacting on your account - via Osko.

### 14.1. Osko overview.

We subscribe to Osko under the BPAY Scheme.

Osko is a secure payment service utilising the New Payments Platform which enables you to send and receive payments in near real-time.

To send a payment via Osko, you don't need to do anything differently, just send the payment via Internet Banking using the 'Pay Anyone' feature and we will route the payment the fastest way possible.

When you send or receive a payment you may see the Osko® logo in your payment confirmation or account transaction history. This indicates that the payment was sent via the New Payments Platform infrastructure using Osko®.

### 14.2. Making Osko payments.

You can make Osko Payments from those of our accounts which support Osko Payments.

To send a payment via Osko the account to which you are sending the payment must be able to receive Osko payments.

If the payee is unable to accept Osko payments but is capable of accepting other types of NPP Payments, we may send the payment as another NPP Payment type. In this case, the timing of making the funds available to the payee is at the discretion of the receiving bank.

If the payee is unable to accept Osko payments or other types of NPP Payment, we will send the payment as a BECS payment. In this case, the timing of making the funds available to the payee will be in accordance with BECS rules and regulations.

Where you make an Osko Payment or other NPP Payment using a credit or debit card, no 'chargeback' rights will be available in relation to the payment.

### 14.3. Transaction limits.

We may impose limits on the value of any Osko Payment, or the aggregate value of Osko Payments or other NPP Payments permitted over a particular period. These limits may be different from limits that apply to other payment types.

### 14.4. Suspension and termination.

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..

We will be required to terminate the Osko service if our right to use 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.

### 14.5. Privacy and confidentiality.

In order to provide you with services under Osko, we may need to disclose your Personal Information to BPAY and/or its Service Providers. If we do not disclose your Personal Information to BPAY or its Service Providers, we will not be able to provide you with services under Osko.

Accordingly, you agree to our disclosing to BPAY, its service providers and such other participants involved in Osko such Personal Information relating to you as is necessary to facilitate the provision of Osko to you.

## 15. Transacting on your account - Online Banking.

### 15.1. ePayments applies to Online Banking and Mobile Banking.

Online Banking is an electronic payment facility and the ePayments Code applies when you transact on your account via Online Banking or Mobile Banking.

Online Banking includes desktop, mobile and tablet banking. Mobile Banking includes your hand held phone.

You can use Online and Mobile Banking to get a better picture of your banking via a desktop, mobile, tablet or phone application. Depending on the features of your account and what device you use, you can:

- see all your accounts on one screen.
- transfer funds between your eligible accounts.
- deposit money into another person's account held at another financial institution or with us.
- pay bills.
- update your details.
- change your password/passcode.
- notify us if you're travelling overseas.
- 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.
- set up and manage one off or regular payments.
- electronically transfer funds to another financial institution.
- electronically transfer funds overseas.
- apply for a 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.
- 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 and transactional account.

- open a term deposit.
- PayTo related functions that a member can access using Online and Mobile Banking.

Fees may apply, for more information refer to the Defence Bank Fees and Charges Schedule.

By using the transfer funds option in Online and Mobile Banking, you may transfer funds between the eligible accounts that are accessible through Online and Mobile Banking.

Further, where you transfer funds after a payment cut-off time on a Business Day or a non-Business Day, that transfer may not be included in the balance of your account for other purposes (such as interest, fees or overdrawing calculations) until the next Business Day.

**15.2. Your secure Online and Mobile Banking login.**

When you log on to Online and Mobile Banking for the first time you will be required to accept these Terms and Conditions that are provided online and change the password we provide you. We may also issue you with a token device and register you with our Secure Code Service to approve transactions in Online Banking. If we do, you will also need that token device or Secure Code.

You may be automatically registered for Online and Mobile Banking when you request to open a new account that is eligible for Online Banking, if not we can provide instructions on how to complete your registration and activate Online Banking.

**15.3. Your secure secondary online banking password.**

Making online changes to account details, to open a product and to remit funds electronically requires the use of a VIP password, the use of a transaction authentication password or the use of 'One time password'.

We will issue you with an initial password to enable you to log into Online Banking. Once you log in, you will need register for 'One time password'.

The 'One time password' is delivered either through secure SMS, or for Defence Personnel the added option of receiving the one time password through a second factor authentication email to your Defence Services email address. We will never ask you for this password. Do not share this password with anyone.

Alternatively, you may also register for VIP Access. Details of which are available on our website at defencebank.com.au.

## 16. Transacting on your account - PayTo.

**16.1. Creating a PayTo Payment Agreement**

**16.1.1.** ePayments Code applies to PayTo Payment Agreements.

**16.1.2.** PayTo allows you to establish and authorise Payment Agreements with merchants or Payment Initiators who offer PayTo as a payment option.

**16.1.3.** If you elect to establish a Payment Agreement with a merchant or Payment Initiator that offers PayTo payment services, you will be required to provide that merchant or Payment Initiator with your personal information including your BSB and account number, or your PayID. You are responsible for ensuring the information you provide to the merchant or Payment Initiator is correct. Any personal information or data you provide to the merchant or Payment Initiator will be subject to their own privacy policy and terms and conditions.

**16.1.4.** Payment Agreements must be recorded in the Mandate Management Service before NPP Payments can be processed in accordance with them. The merchant or Payment Initiator is responsible for creating and submitting a record of each Payment Agreement to their financial institution or payments processor for inclusion in the Mandate Management Service. The Mandate Management Service will notify us of the creation of any Payment Agreement established using your account or PayID details. We will notify you of the creation of a Payment Agreement, and provide details of the merchant or Payment Initiator, the payment amount and payment frequency (if these are provided) to seek your confirmation of the Payment Agreement. You may confirm or decline any Payment Agreement presented for your approval. If you confirm, we will record your confirmation against the record of the Payment Agreement in the Mandate Management Service and the Payment Agreement will then be effective. If you decline, we will note that against the record of the Payment Agreement in the Mandate Management Service.

**16.1.5.** We will only process payment instructions in connection with a Payment Agreement once you have confirmed the Payment Agreement and it is effective. Once the Payment Agreement is effective we will process payment instructions received from the merchant's or Payment Initiator's financial institution. We are not liable for any loss you or any other person may suffer as a result of our processing a payment instruction submitted under a Payment Agreement that you have confirmed.

**Payment instructions may be submitted to us for processing immediately after you have confirmed the Payment Agreement so you must take care to ensure the details of the Payment Agreement are correct before you confirm them.**

**16.1.6.** If a Payment Agreement requires your confirmation within a timeframe stipulated by the merchant or Payment Initiator, and you do not provide confirmation within that timeframe, the Payment Agreement may be withdrawn by the merchant or Payment Initiator.

**16.1.7.** If you believe the payment amount or frequency or other detail presented is in incorrect, you may decline the Payment Agreement and contact the merchant or Payment Initiator and have them amend and resubmit the Payment Agreement creation request.

**16.1.8.** This Section 16.1 does not apply to Migrated DDR Mandates.

**16.2. Amending a Payment Agreement**

**16.2.1.** Your Payment Agreement may be amended by the merchant or Payment Initiator from time to time, or by us on your instruction.

**16.2.2.** We will notify you of proposed amendments to a Payment Agreement requested by the merchant or Payment Initiator. Such amendments may include variation of the payment amount (if a fixed amount) or payment frequency. You may confirm or decline any amendment request presented for your approval. If you confirm, we will record the confirmation against the record of the Payment Agreement in the Mandate Management Service and the amendment will then be effective. If you decline, the amendment will not be made and the Payment Agreement will continue on existing terms.

**16.2.3.** If you do not confirm or decline an amendment request within 5 calendar days of it being sent to you, then the amendment request will be deemed to be declined.

**16.2.4.** If you decline the amendment request because it does not reflect the updated terms of the agreement that you have with the merchant or Payment Initiator, you may contact them and have them resubmit the amendment request with the correct details. We are not authorised to vary the details in an amendment request submitted by the merchant or Payment Initiator.

**16.2.5.** Once an amendment request has been confirmed by you, we will promptly update the Mandate Management Service with this information.

**16.2.6.** Once a Payment Agreement has been established, you may instruct us to amend your name or transfer the Payment Agreement to another account you hold with us. If you wish to transfer the Payment Agreement to an account with another financial institution, you may give us a transfer instruction (see Section 16.4 "Transferring your Payment Agreement"). We may decline to act on your instruction to amend your Payment Agreement if we are not reasonably satisfied that your request is legitimate. You may not request us to amend the details of the merchant or Payment Initiator, or another party.

**16.3. Pausing your Payment Agreement**

**16.3.1.** You may instruct us to pause and resume your Payment Agreement. We will act on your instruction to pause or resume your Payment Agreement promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption. While the Payment Agreement is paused, we will not process payment instructions in connection with it. We are not liable for any loss that you or any other person may suffer as a result of you pausing a Payment Agreement.

**Before pausing a Payment Agreement you should ensure this will not breach, or result in a breach of, any contract you have with the merchant or Payment Initiator.**

**16.3.2.** A merchant or Payment Initiator may pause and resume a Payment Agreement to which you are a party, in which case we will promptly notify you of that pause or subsequent resumption. We are not liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement by the merchant or Payment Initiator.

**16.4. Transferring your Payment Agreement**

**16.4.1.** When available, you may ask us to initiate the transfer of a Payment Agreement to an account at another financial institution. We will provide you with a Transfer ID to provide to your new financial institution to enable them to complete the transfer.

**16.4.2.** Your new financial institution will be responsible for obtaining your consent to transfer the Payment Agreement and for updating the Payment Agreement in the Mandate Management Service. The updated Payment Agreement will only become effective upon being updated in the Mandate Management Service.

**16.4.3.** Until the transfer is completed, the Payment Agreement will remain linked to your account with us and payments under the Payment Agreement will continue to be made from your account with us. If the other financial institution does not complete the transfer within 14 calendar days, the transfer will be deemed to be ineffective and payments under the Payment Agreement will continue to be made from your account with us.

**16.4.4.** To transfer a Payment Agreement that you have with another financial institution to us, you will need to obtain a Transfer ID from that institution and provide it to us. We will use reasonable endeavours to process the transfer within 14 calendar days. Not all Payment Agreements will be transferrable to us. If we are unable to complete a transfer, we will notify you and advise you of your options.

**16.5. Cancelling your Payment Agreement**

**16.5.1.** You may instruct us to cancel a Payment Agreement on your behalf. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancelling a Payment Agreement.

**You may remain liable to the merchant or Payment Initiator for payments that would otherwise have been paid under the Payment Agreement, including for any cancellation fees.**

**16.5.2.** A merchant or Payment Initiator may cancel a Payment Agreement to which you are a party, in which case we will promptly notify you of that cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancellation of your Payment Agreement by the merchant or Payment Initiator.

**16.6. Migration of Direct Debit arrangements**

**16.6.1.** A merchant or Payment Initiator who has an existing direct debit arrangement with you, may migrate it to a Payment Agreement, as a Migrated DDR Mandate. We are not obliged to notify you of a Migrated DDR Mandate. We will process instructions received from a merchant or Payment Initiator on the basis of a Migrated DDR Mandate.

**A Migrated DDR Mandate takes effect without your confirmation. If you do not consent to the migration of a direct debit arrangement you should contact the merchant or Payment Initiator.**

**16.6.2.** A Migrated DDR Mandate has effect as a Payment Agreement. You may amend, pause (and resume), cancel or transfer your Migrated DDR Mandates, and will receive notice of amendment, pause or resumption, or cancellation initiated by the merchant or Payment Initiator of your Migrated DDR Mandates, in the same manner as for other Payment Agreements.

**16.7. General PayTo Provisions**

**16.7.1.** A Payment Agreement can only be linked to an account that has the PayTo facility.

**16.7.2.** You must carefully consider any Payment Agreement creation request, or amendment request made in respect of a Payment Agreement, and promptly respond to such requests. We are not liable for any loss that you suffer as a result of any payment processed by us in accordance with the terms of a Payment Agreement.

**16.7.3.** You must notify us immediately if you no longer hold or have authority to operate the account from which a payment under a Payment Agreement has been or will be made.

**16.7.4.** You must promptly respond to any notification that you receive from us regarding the pausing or cancellation of a Payment Agreement for misuse, fraud or for any other reason. We are not responsible for any loss that you suffer as a result of you not promptly responding to such a notification.

**16.7.5.** You are responsible for complying with the terms of any agreement that you have with a merchant or Payment Initiator, including any termination notice periods. You are responsible for any loss that you suffer in connection with you cancelling or pausing a Payment Agreement, including for a breach of any agreement that you have with that merchant or Payment Initiator.

**16.7.6.** You are responsible for ensuring that you have sufficient funds in your account to meet the requirements of all your Payment Agreements. We are not responsible for any loss that you suffer as a result of your account having insufficient funds to meet a payment instruction under a Payment Agreement. See Section 4.9 "Overdrawing your account?" for our rights if there are insufficient funds in your account.

**16.7.7.** If you receive a Payment Agreement creation request or become aware of payments being processed from your account that you are not expecting or experience any other activity that appears suspicious or erroneous, please report such activity to us immediately.

**16.7.8.** From time to time we may ask you to confirm that your Payment Agreements are accurate and up to date. You must promptly respond to any such request. Failure to respond may result in us pausing the Payment Agreements.

**16.7.9.** We recommend that you allow notifications from the Defence Bank App to your mobile device to ensure that you're able to receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way.

**16.7.10.** You are responsible for ensuring that: (i) all data you provide to us or to any merchant or Payment Initiator that subscribes to PayTo is accurate and up to date; (ii) you do not use PayTo to send threatening, harassing or offensive messages to the merchant, Payment Initiator or any other person; and (iii) any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.

**16.7.11.** All intellectual property, including but not limited to the PayTo trade marks and all documentation, remains our property, or that of our licensors (Our Intellectual Property). We grant to you a royalty free, non-exclusive license (or where applicable, sub-license) for the Term to use Our Intellectual Property for the sole purpose of using PayTo in a way that is consistent with these terms and conditions.

**16.7.12.** Where an intellectual property infringement claim is made against you, we will have no liability to you under this agreement to the extent that any intellectual property infringement claim is based upon: (i) modifications to Our Intellectual Property by or on behalf of you in a manner that causes the infringement; (ii) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item; (iii) your failure to use corrections or enhancements to Our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and (iv) your failure to use Our Intellectual Property in accordance with this agreement.

**16.7.13.** We may cancel or suspend your use of PayTo in accordance with our rights under Section 4.16 "Suspension or termination of accounts and services.".

**16.7.14.** We may amend the terms and condition relating to PayTo in accordance with our rights under Section 19.1 "What changes can the bank make to my account?". If you do not accept our amendments, you may cease using PayTo.

**16.7.15.** You must comply with all applicable laws in connection with your use of PayTo.

**16.7.16.** We will accurately reflect all information you provide to us in connection with a Payment Agreement in the Mandate Management Service.

**16.7.17.** We may monitor your Payment Agreements for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreements if we reasonably suspect misuse, fraud or security issues. We will promptly notify you of any such action.

**16.7.18.** If you become aware of a payment being made from your account, that is not permitted under the terms of your Payment Agreement or that was not authorised by you, contact us immediately and submit a claim. We will promptly respond to all claims and if the claim is founded, we will refund your account. We are not liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement.

**16.7.19.** We may impose daily, or other periodic, limits on the value of payments that can be made using PayTo. We may reject any payment instructions from a merchant or Payment Initiator that will cause you to exceed any such limit. We are not liable for any loss that you or any other person may suffer as a result of us rejecting a payment instruction under this Section 16.7.19.

**16.7.20.** If your Payment Agreement is linked to a PayID:

- transferring your PayID to another [financial institution]/[account (whether with us or another financial institution)] will not automatically transfer the Payment Agreement to that [financial institution]/[account], and payments under the linked Payment Agreement will fail (subject to Section 16.7.21);
- closing your PayID will cause payments under the linked Payment Agreement to fail (subject to Section 16.7.21).

**16.7.21.** To ensure payments under a linked Payment Agreement continue after transferring or closing the PayID you will also need to either link the Payment Agreement to an account with us (see Section 16.2 "Amending a Payment Agreement") or transfer the Payment Agreement to another financial institution (see Section 16.4 "Transferring your Payment Agreement").

### 16.8. Privacy and PayTo

**16.8.1.** By confirming a Payment Agreement or permitting the creation of a Migrated DDR Mandate against your account with us, you acknowledge that you authorise us to collect, use and store your personal information and the details of your Payment Agreement or Migrated DDR Mandate in the Mandate Management Service, and that these details may be disclosed to the financial institution or payment processor for the merchant or Payment Initiator, for the purposes of creating payment instructions and constructing NPP Payment messages and enabling us to make payments from your account.

### 16.9. Authority for PayTo Instructions

**16.9.1.** Your instructions in relation to a Payment Agreement must be provided in accordance with the account operating instructions for the account that is, or is intended to be, linked to the Payment Agreement. This includes instructions to confirm or decline a Payment Agreement or the merchant's or Payment Initiator's amendments to a Payment Agreement, or to amend, pause, resume, cancel or transfer a Payment Agreement. For example, instructions to confirm a Payment Agreement linked to a joint account operated jointly must be provided jointly.

## 17. Your rights, obligations and liability when using an electronic payment facility.

This section applies to payments, funds transfer and cash withdrawal transactions provided by us that are:

(a) initiated using electronic equipment, and

(b) not intended to be authenticated by comparing a manual signature with a specimen signature.

### 17.1. What are electronic transactions?

The following are electronic transactions:

- online banking.
- mobile banking.
- BPAY®.
- electronic card transactions.
- osko.
- direct debits.
- direct credits.
- auto transfers.
- PayTo payments.

### 17.2. Third party electronic transactions.

Where a payment facility is provided by a third party your rights are governed by their terms and conditions of service.

### 17.3. ePayments Code.

We subscribe to the ePayments Code.

The ePayments Code regulates electronic transactions.

The ePayments Code 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.

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

### 17.4. Your security.

We care as much about your money as you do. Here are some helpful hints on how to protect your electronic banking to protect the security of any access device such as a PC, mobile phone or mobile device.

- keep up to date anti-virus, anti-spyware, firewall software.
- change your passwords on a regular basis.
- password strength - use more complex passwords, such using alphanumeric characters to reduce the risk of unauthorised access to your account.

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.

### 17.5. Guidelines for protecting your accounts, passwords and passcodes.

Security on your account is important to us so please look at the suggestions below on how to protect your account so other people can't use it. The below are guidelines only. Your liability for losses resulting from unauthorised transactions will be determined by the ePayments Code. For Visa Debit card related security you should refer to the Visa Debit card Conditions of Use.

If you think someone else knows your passcode or password or has used your account, let us know straight away. If you don't, you may be responsible for any financial losses (see section 4).

**Do:**

- memorise your passcode or password as soon as possible, then destroy or delete it.
- immediately report the loss, theft of funds from your account(s) due to unauthorised transactions.
- immediately notify us of any change of address.
- examine your periodical statement immediately upon receiving it to identify any unusual transactions and then report them to us as soon as possible.
- review your transaction history in online banking or the App to identify any unusual transactions and then report them to us soon as possible.
- use care to prevent anyone seeing the passcode or password when using digital channels, e.g. mobile banking application or internet banking.

**Don't:**

- write down your passcode or password.
- keep a copy of your passcode or password on your computer, mobile or tablet.
- tell your passcode or password to anyone - not even family or friends.
- use a number or word that someone can easily guess (for example, your date of birth, '1234' or 'password').
- let anyone see your passcode when you're using it.

For Visa Debit card terms and conditions relating to PIN protection refer to our Visa Debit card Conditions of Use document.

**17.6. Passcode security requirements.**

**17.6.1.** This section applies where one or more passcodes are needed to perform a transaction.

**17.6.2.** A user must not:

(a) voluntarily disclose one or more passcodes to anyone, including a family member or friend,

(b) where a device is also needed to perform a transaction, write or record passcode(s) on a device, or keep a record of the passcode(s) on anything:

(i) carried with a device, or

(ii) liable to loss or theft simultaneously with a device,

unless the user makes a reasonable attempt to protect the security of the passcode, or

(c ) where a device is not needed to perform a transaction, keep a written record of all passcodes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the passcode(s).

**17.6.3.** As a guide, a reasonable attempt to protect the security of a passcode record includes making any reasonable attempt to disguise the passcode within the record, or prevent unauthorised access to the passcode record, including by:

(a) hiding or disguising the passcode record among other records,

(b) hiding or disguising the passcode record in a place where a passcode record would not be expected to be found,

(c) keeping a record of the passcode record in a securely locked container, or

(d) preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

**17.6.4.** A user must not act with extreme carelessness in failing to protect the security of all passcodes/passwords where extreme carelessness means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour.

**17.6.5.** A user must not select a numeric passcode/password that represents their birth date, or an alphabetical passcode/password that is a recognisable part of their name. If you do use an obvious passcode/password such as a name or date you may be liable for any losses which occur as a result of unauthorised use of the passcode/password before notification to us that the passcode/password has been misused or has become known to someone else.

**17.7. Process for investigating a report of an unauthorised transaction**

If you report an unauthorised transaction, reasonable efforts will be made to obtain the following information:

(a) the type of facility,

(b) where relevant, any identifiers,

(c) the type of device and/or passcode used to perform the transaction,

(d) the name and address of the holder,

(e) the name of other user(s),

(f) whether a device used to perform the transaction was signed by the user,

(g) whether a device was lost, stolen or misused or the security of a passcode was breached, and if so: (i) the date and time of the loss, theft or misuse of the device, or breach of passcode security,

(ii) the date and time the loss, theft or misuse of the device, or breach of passcode security, was reported to the subscriber, and

(iii) the date, time and method of reporting the loss, theft or misuse of the device, or breach of passcode security, to the police,

(h) where one or more passcodes were required to perform transactions, whether the user recorded the passcode(s), and if so:

(i) how the user recorded the passcode(s),

(ii) where the user kept the record, and

(iii) whether the record was lost or stolen,and, if so, the date and time of the loss or theft,

(i) where one or more passcodes were required to perform transactions, whether the user had disclosed the passcode(s) to anyone,

(j) details of where and how the loss, theft or misuse of a device, or breach of passcode security, occurred (for example,housebreaking, stolen wallet),

(k) details of the transaction to be investigated, including:

(i) a description,

(ii) the date and time,

(iii) the amount, and

(iv) the type and location of electronic equipment used,

(l) details of any surrounding circumstances,

(m) any steps taken by the user to ensure the security of any device or passcode(s)needed to perform transactions that the user considers relevant to the liability of the holder, and

(n) details of the last authorised transaction performed using the facility.

**Timeframes**

- Within 21 days of receiving a report of an unauthorised transaction, we will:

  (a) complete the investigation and advise you, in writing, of the outcome, or

  (b) advise you in writing of the need fo rmore time to complete the investigation.

- Unless there are exceptional circumstances, we will complete the investigation within 45 days of receiving the report of an unauthorised transaction.

- We will respond to requests for information from other subscribers within 15 days, unless there are exceptional circumstances.

**Explaining the outcome of a report of an unauthorised transaction**

- We will tell the person who reports an unauthorised transaction:

  (a) the outcome of the report, and

  (b) the reasons for the outcome, including references to the relevant clauses of the ePayments code.

  Where we are subject to Appendix A of the ePayments code and decide that you are partly or wholly liable for a transaction under Chapter C of the ePayments code, we must:

  (a) give you copies of any documents or other evidence, including information about the transaction from any logs or audit trails, and

  (b) advise the holder, in writing, whether there was any system or equipment malfunction at the time of the transaction.

  **17.7.1.** If a report of an unauthorised transaction is settled to the complete satisfaction of you and the us within 5 business days, we are not required to advise you in writing of the outcome of the report, unless you request a written response.

**17.8. When you are not liable for loss arising from unauthorised electronic transactions.**

You are not liable for loss arising from an unauthorised electronic transaction if the cause of the loss is any of the following:

- fraud or negligence by our employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent.
- a device, identifier or passcode which is forged, faulty, expired or cancelled.
- a transaction requiring the use of a device and/or passcode that occurred before the user received the device and/or passcode (including a reissued device and/or passcode).
- a transaction being incorrectly debited more than once to the same account.
- an unauthorised transaction performed after we have been informed that a device has been misused, lost or stolen, or the security of a passcode/password has been breached.

You are not liable for loss arising from an unauthorised transaction that can be made using an identifier without a passcode/password or device. Where a transaction can be made using a device, or a device and an identifier, but does not require a passcode, you are liable only if the user of the device unreasonably delay in reporting the loss or theft of the device.

You are not liable for loss arising from an unauthorised transaction where it is clear that a user has not contributed to the loss.

In a dispute about whether a user has received a device or passcode/password:

- there is a presumption that the user did not receive it, unless we can prove that you or your nominee did receive it.
- we can prove that a user received a device or passcode by obtaining an acknowledgement of receipt from the user.
- we may not rely on proof of delivery to a user's correct mailing or electronic address as proof that the user received the device or passcode.

**17.9. When you are liable for loss arising from unauthorised electronic transactions.**

You may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this sub clause.

Where we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching our passcode/password security requirements:

- you are liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of passcode/password security is reported to us.
- you are not liable for the portion of losses:
  - incurred on any one day that exceeds any applicable daily transaction limit.
  - incurred in any period that exceeds any applicable periodic transaction limit.
  - that exceeds the balance on the facility, including any pre-arranged credit.
  - incurred on any facility that we and you had not agreed could be accessed using the device or identifier and/or passcode used to perform the transaction.

  **Where:**

  - more than one passcode/password is required to perform a transaction and
  - we prove that a user breached our passcode/password security requirements for one or more of the required passcodes/passwords, but not all of the required passcodes/passwords you are liable under this section only if we also prove on the balance of probability that the breach of our passcode/password security requirements was responsible for the losses, when assessed together with all the contributing causes.

You are liable for losses arising from unauthorised transactions that occur because a user contributed to losses by leaving a card in an ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM. (Note: Reasonable safety standards that mitigate the risk of a card being left in an ATM include ATMs that capture cards that are not removed after a reasonable time and ATMs that require a user to swipe and then remove a card in order to commence a transaction).

Where we can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a device, or that the security of all passcodes/password has been breached, you:

- are liable for the actual losses that occur between:
  - when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and
  - when the security compromise was reported to us.
- are not liable for any portion of the losses:
  - incurred on any one day that exceeds any applicable daily transaction limit.
  - incurred in any period that exceeds any applicable periodic transaction limit.
  - that exceeds the balance on the account including any pre-arranged credit.
  - incurred on any account that we and you had not agreed could be accessed using the device and/or passcode used to perform the transaction.

Where a passcode/password was required to perform an unauthorised transaction, and the preceding paragraphs of this sub clause do not apply, you are liable for the lower of:

- $150, or a lower figure determined by us;
- the balance of the account which we and you have agreed can be accessed using the device and/or passcode/password, including any pre-arranged credit.
- the actual loss at the time that the misuse, loss or theft of a device or breach of passcode/password security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.

In deciding whether on the balance of probabilities we have proved that a user has contributed to losses as stated in the preceding paragraphs of this sub clause:

- we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring.
- the fact that an account has been accessed with the correct device and/or passcode, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of our passcode/password security requirements.
- the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example, the number and expiry date of a device) is not relevant to a user's liability.

If a user reports an unauthorised transaction on a card account, or charge card account we will not hold you liable for losses for an amount greater than your liability if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, chargeback rights).

This section does not require us to exercise any rights we may have under the rules of a card scheme. However, we cannot hold you liable under this section for a greater amount than would apply if we had exercised those rights.

**17.10. Liability for loss caused by system or equipment malfunction.**

You are not liable for loss caused by the failure of a system or equipment provided by any party to a shared electronic network to complete a transaction accepted by the system or equipment in accordance with a user's instructions.

Where a user should reasonably have been aware that a system or equipment provided by any party to a shared electronic network was unavailable or malfunctioning, our liability is limited to:

- correcting any errors.
- refunding any fees or charges imposed on the user.

**17.11. Availability.**

Most Defence Bank accounts come with internet banking and Mobile banking access. If you haven't already activated your internet banking mobile banking app and wish to gain access to these facilities, contact us to do so.

If you believe that your PIN(s) or, passcode or password(s) for telephone, internet banking or mobile app have become known to someone else, been misused, lost or stolen you must contact us immediately and change them.

**17.12. Mistaken payments.**

A mistaken payment is where you have entered some incorrect details, such as account number, BSB or PayID but does not include payments made by BPAY.

**17.12.1. What is a mistaken internet payment?**

A mistaken internet payment is a payment made by a user through a 'Pay Someone' internet banking facility and processed by an authorised deposit-taking institution (ADI) through the BECS direct entry system where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:

- the user's error, or
- the user being advised of the wrong BSB number and/or identifier.

This does not include payments made using BPAY or PayTo.

The provisions of this clause do not apply to payments made via the New Payments Platform but we will endeavour to assist you in relation to such payments where you or another user pays funds to an unintended recipient.

A mistaken internet payment may apply where you or another user pays funds to an unintended recipient or you are in receipt of funds from a user and that user asserts that you are the unintended recipient of the funds.

**17.12.2. What is a misdirected payment?**

A misdirected payment is a payment made by a user using a PayID where funds are paid into the account of an unintended recipient because the PayID wasn't correctly created or maintained by the recipient's ADI.

**17.12.3. What you should do if you believe you have made a mistaken or misdirected payment.**

If you believe you have made a mistaken payment or a misdirected payment you should report the matter to us.

**17.12.4. What we do when you report a mistaken payment or a misdirected payment.**

When you report a mistaken payment, we must investigate whether a mistaken payment has occurred.

If we are satisfied that a mistaken internet payment has occured, we must send the receiving ADI a request as soon as reasonably possible and by no later than 5 business days for the return of funds.

If we are satisfied that a mistaken payment has occurred but the payment was made via the New Payment Platform, we will assist you by sending a request to the receiving ADI a request for the return of the funds, but the receiving ADI is not obliged to respond to or act on our request.

The receiving ADI must within 5 business days of receiving a request for the return of the funds in connection with a mistaken internet payment:

- acknowledge the request for the return of funds, and
- advise us whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

We must inform you of the outcome of the reported mistaken internet payment in writing and within 30 business days of the day on which the report is made.

If we are not satisfied that a mistaken internet payment has occurred, we will not take any further action.

#### 17.12.5. What to do if you are not satisfied with the outcome of your mistaken internet payment request.

You may complain to us about how the mistaken payment report has been dealt with, including that we and/or the receiving ADI:

- is not satisfied that a mistaken internet payment has occurred.
- have not complied with the processes and timeframes set out in the preceding paragraphs section.

If we receive a complaint we must:

- deal with the complaint under our internal dispute resolution procedures.
- not require you to complain to the receiving ADI.

If you are not satisfied with the outcome of a complaint you make, then you are entitled to lodge a complaint with our external dispute resolution scheme provider, Australian Financial Complaints Authority. Refer to the Complaints section for AFCA contact details and further information.

#### 17.12.6. Mistaken payments into your account.

Where someone alleges that they made a mistaken payment into your account we are obliged in the circumstances set out in the ePayments Code to deal with any requests made to refund those amounts and debit your account. In that circumstance we are the "receiving ADI and we are required to act in accordance with table above headed "Information about a receiving ADI's obligations after we request return of funds".

Any deposits into your account are accepted on the basis that we may be required to refund the deposit in terms of the ePayments Code and you agree to us acting in accordance with those and further agree not to make any claim against us in these circumstances.

#### 17.12.7. Over payments.

An overpayment is not a Mistaken Internet Payment. If you make an internet payment and later discover that the amount you paid was greater than the amount you needed to pay, you must contact the payee if you wish to obtain a refund.

#### 17.12.8. Misdirected payments.

Misdirected payments are where the payment goes astray because the intended recipients bank miscodes the Pay ID of its customer. In those circumstances you we may assist however are not required to seek recovery.

## 18. Account administration.

### 18.1. What changes can the bank make to my account?

We may change fees, charges interest rates and other conditions on your account, but in most cases, we will let you know before the change is implemented.

The following table sets out the minimum notice period we will provide you prior to any change being implemented. This does not apply to a change to, or introduction of, a government charge (see Section 4.19). If you have questions or concerns about the change you should contact us, otherwise your use of the account after the expiry of the notice period is deemed acceptance by you of the changes contained in that notice.

As interest rates can change regularly, we avoid 'spamming' you with updates on this and instead update them on our website as they change.

| Type of change. | Minimum notice period. |
|---|---|
| Increasing any fee or charge. | 30 days. |
| Adding a new fee or charge. | 30 days. |
| Reducing the number of fee-free transactions permitted on your account. | 30 days. |
| Changing the minimum balance to which an account keeping fee applies. | 30 days. |
| Changing the method by which interest is calculated. | 30 days. |
| Changing the circumstances when interest is credited to your account. | 30 days. |
| Changing deposit interest rates. | On the day of change. |
| Increasing your liability for losses relating to ePayments. | 30 days. |
| Imposing, removing or changing any periodic transaction limit. | 30 days. |
| Changing any other term or condition. | Before the change or event occurs or as soon as practicable after, but not more than 6 months after, the change or event occurs. |

We may use various methods, and combinations of methods, to notify you of these changes, such as:

- by letter, email or other direct communication.
- on or with your next statement of account.
- on or with the next newsletter.
- advertisements in the local or national media notification on our website.

We will always select a method(s) appropriate to the nature and extent of the change, as well as the cost effectiveness of the method of notification.

## 19. Round Ups.

Defence Bank Round Ups is an optional feature which helps you to save by rounding up the value of certain transactions made with a Visa Debit, and automatically transferring the 'Round Up Amount' to your savings account. By making a purchase on your card, we deduct (rounded to the selected nearest dollar value) from your 'Eligible Accounts' and add to your savings accounts.

For details of 'Eligible accounts', refer to the Summary of accounts and access facilities document under 'Round Ups debits.

Your Round Up can be transferred 'to' any of our savings and transactional accounts.

### 19.1. How it works.

When you activate Defence Bank Round Ups, you can round up each eligible transaction to the nearest $1.00, $5.00 or $10.00 amount.

For example, Mary has her Round Ups set to $1.00 and buys a Coffee for $3.50 with her Defence Bank Visa Debit card which is attached to her Everyday Access account.

We will debit the purchase amount of $3.50 from her Everyday Access and transfer an additional $0.50 (the Round Up Amount) from her Everyday Access account to her Max eSaver.

The total deduction 'rounded' from the Everyday Access account is $4.00.

The total transfers to Mary's chosen Round Up account, the Max eSaver is $0.50

**19.2. How to start rounding up.**

(1) Have an Eligible Account and a Visa Debit card with us.

(2) You'll also need a second account to connect your Round Up to. This can be any of our savings and transactional accounts, for example you may nominate your Max eSaver or iSaver account.

(3) Log into the Defence Bank App and select Round Up from the side menu.

Follow the onscreen instructions and select your transaction account and the account you would like to start rounding up to. For more information visit our website and search 'Round Ups'.

**19.3. A Round Up will work when.**

(1) You use your Visa Debit card connected to your Eligible account (which may have an overdraft facility attached). This includes in-store transactions, payWave and digital wallet; or

(2) You make an online purchase with your Visa Debit card.

(i) Processing the Round Up Amount.

Each Round Up Amount will be:

- debited from your Eligible Account and transferred to your savings account in a separate transaction which will ordinarily occur when the visa transaction is settled. It can be days after the eligible purchase is made (e.g. in store, when making the purchase online), but in some circumstances may be processed up to 2 hours after the eligible purchase is made; and
- credited to your savings account as a separate transaction.

**19.4. Stopping or editing your Round Up.**

The Round Up Amount will not be debited if doing so will cause your account to be overdrawn, or if the Account is already overdrawn.

(ii) Merchant Reversals.

If a transaction debited to your Account is reversed by the merchant, the transfer of the Round Up Amount related to that transaction will not be reversed.

(iii) Changes.

You can change your selected Round Up Amount or your nominated savings account at any time via Mobile Banking. Any such change will take effect promptly.

(iv) Disabling the Defence Bank Round Up feature via the Defence Bank App, the same location where you first set up your Round Ups.

The Defence Bank Round Up feature may be withdrawn at any time if:

- your nominated Eligible Account is closed;
- there is a material breach of the Account Terms by you; or
- we are otherwise authorised by law or compelled by our compliance arrangements to do so.

We will notify you when this occurs.

For more information on how to stop or edit your Round Up feature visit our website.

## 20. Your rights and obligations.

### 20.1. Financial difficulty.

We understand that life is unpredictable and circumstances can change.

A variety of life events and changes to circumstance can put a significant strain on your finances and make it difficult to meet your financial obligations - but we're here to help.

If you get into financial difficulty, the sooner you let us know, the sooner we can work with you to help you get back on your feet.

Our Member care team are available to help you. You can either:

- Call our Contact Centre on 1800 003 139
- Talk to a consultant at any of our branches
- Visit our website defencebank.com.au and search "financial hardship".

### 20.2. Complaints.

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

**How to make a complaint and the complaints process.**

If you have a complaint, you can lodge this with us via one of the following methods:

- by visiting your local branch
- calling our Contact Centre on 1800 033 139
- emailing info@defencebank.com.au (for the attention of the Complaints Officer)
- sending us a direct message on one of our social media channels, including Facebook, Twitter, Instagram or LinkedIn.
- writing to us at the following address:

The Complaints Officer
Defence Bank
PO Box 14537
Melbourne VIC 8001

In lodging a complaint with us, we will usually need your full name, member number (if applicable), contact details, a short description of your complaint and your desired resolution for us to help you.

If you need further help with the complaints process, contact us using any of the above channels and we will try to assist you.

**Keeping you informed.**

When you lodge a complaint with us, we will acknowledge this to you within one business day of receiving this. We will provide this to you either at the time you lodge your complaint or via the channel that you have indicated as your preferred method of communication.

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

Based upon our investigation, we will advise you of the outcome of our investigation into your complaint and the reasons for our decision within 30 days.

In certain circumstances, the timeframe for us to investigate and respond to a complaint will vary from the 30 day period outlined above. Should this apply to your particular complaint, we will advise you of this at the time we acknowledge receipt of your complaint.

In advising you of the outcome of our investigation, the response provided to you in writing will include the following:

- the reasons for the decision
- the information that was reviewed to assist in determining our decision
- the further actions that Bank has or may take in response to the complaint raised
- further action you may consider taking in response

**Still not satisfied?**

If you are not satisfied with the final outcome of your complaint, or if we fail to resolve your complaint within 30 days, you may pursue the matter further with the Australian Financial Complaints Authority (AFCA).

You can submit a complaint to the Australian Financial Complaints Authority via one the following methods:

- on their website at www.afca.org.au
- by emailing them at info@afca.org.au
- in writing to:

Australian Financial Complaints Authority
GPO Box 3
Melbourne VIC 3001

- by calling them on 1800 931 678

**20.3. Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF).**

**20.3.1** So that we can meet our legal and regulatory obligations under AML/CTF Laws, we must exercise a level of control and monitoring over accounts and access facilities opened with Defence Bank. This means that we may delay, freeze, block or refuse to make or receive any payment using the services detailed in these Conditions of Use if we believe on reasonable grounds that making, receiving or crediting the payment may breach any law in Australia or any other country, and we will incur no liability to you if we do so. When you open an account with us you agree that:

**20.3.2** where required, you will provide to us all information reasonably requested in order for us to comply with our obligations under AML/CTF Legislation or the Visa Scheme Rules;

**20.3.3** to meet our regulatory obligations, we may require that you provide us with additional information. You should be aware that where we are obliged to do so we will disclose the information gathered to regulatory and/or law enforcement agencies, other banks, payment system participants, service providers and other third parties.

**20.3.4** we or Cuscal may block, delay, freeze or refuse any transactions where we have reason to believe that the relevant transactions are fraudulent, in breach of the AML/ CTF Legislation, the Visa Scheme Rules or any other relevant laws;

**20.3.5** where transactions are blocked, delayed, frozen or refused by us in accordance with this section, you agree that we are not liable for any loss suffered arising directly or indirectly as a result of us taking this action; and

**20.3.6** we will monitor all transactions that arise pursuant to your use of the VISA Debit card in accordance with our obligations under AML/CTF Legislation and the Visa Scheme Rules.

**20.4. Accuracy of information.**

We do not warrant that:

- the information available to you about your accounts through our internet banking service is always up to date.
- you will have 24 hours a day, 7 days per week, access to internet banking data you transmit via internet banking is totally secure.

**20.5. Copies of documents, statements and other information.**

At your request we will send you, or make available to you, a copy of any of the following documents relating to a product or facility you have, or have had, with us:

- a loan application.
- a contract (including standard Terms and Conditions, and details of interest rates and fees and charges).
- a mortgage or other security document, an account statement; and
- a notice we have previously given you about us exercising our rights (unless the request is for a notice issued more than two years before the discharge or termination of the contract to which the notice is related).

This section does not apply to documents we are no longer legally required to retain.

If a copy of a document is requested, we will provide it, or make it available, to you:

- within 14 days, if the original came into existence 1 year or less before you make the request, and
- within 30 days, if the original came into existence more than 1 year but less than 7 years before you make the request. If for some reason we are unable to provide a document within these timeframes, we will advise you in writing, together with the expected timeframe for providing the document.

Documents may be provided in electronic form, in the form of a computer-generated record, or in any other form as mutually agreed.

We may charge a reasonable fee, reflecting our costs, for providing a document.

Access to your personal information is considered more generally in section 23.

### 20.6. Consequential damage for payments.

This section does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed (including the ePayments Code and the Customer Owned Banking Code of Practice). If those laws would make this section illegal, void or unenforceable or impose an obligation or liability which is prohibited by those laws or that code, this section is to be read as if it were varied to the extent necessary to comply with those laws or that code or, if necessary, omitted.

We are not liable for any consequential loss or damage (including any loss of profit) you suffer as a result of your use of any access method (such as BPAY, Osko, PayTo, EFTPOS, VISA Debit card and direct debits) for sending or receiving, or arranging to send or receive any payments from your account, other than loss due to our negligence or in relation to any breach of a condition or warranty implied by the law of contracts for the supply of goods and services which may not be excluded, restricted or modified at all, or only to a limited extent. However, for transactions governed by the ePayments Code, we do not deny your right to claim consequential damages resulting from a malfunction of a system or equipment provided by a party to a shared electronic payments network that you are entitled to use pursuant to these Conditions of Use except where a user should reasonably have been aware that the system or equipment was unavailable or malfunctioning, in which case our liability is limited as set out in section 18.10.

In respect of any warranty or consumer guarantee which is unable to be excluded under any relevant law, our liability in respect of a breach of that warranty or guarantee relating to your use of account is limited to the re-supply of the services or the payment of the cost of having the services supplied again at your discretion.

## 21. Protecting your money.

### 21.1. Financial claims scheme.

When you acquire any of our deposit products described in this DPS and in our **Summary of Accounts and Access Facilities** document you will be covered by the Financial Claims Scheme (FCS).

The Financial Claims Scheme 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 of 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 www.apra.gov.au or by phone on 1300 55 88 49, or on +61 2 8037 9015 if calling from overseas.

### 21.2. Customer Owned Banking Association Code of Banking Practice.

We are subscribing member to the Customer Owned Banking Code of Practice.

The Customer Owned Banking code of practice is for Australia's customer-owned banking institutions which has been developed in close consultation with a wide range of stakeholders, including government and consumer groups.

At Defence Bank, our members can have the confidence in knowing they are covered by a bank committed to fair, secure and responsible banking.

In alignment with the Customer Owned Banking Code of Practice our 10 key promises to you are:

- we will be fair and ethical in our dealings with you.
- we will focus on our customers.
- we will give you clear information about our products and services.
- we will be responsible lenders.
- we will deliver high customer service and standards.
- we will deal fairly with any complaints.
- we will recognise your rights as owners.
- we will comply with our legal and industry obligations.
- we will recognise our impact on the wider community.
- we will support and promote the Customer Owned Banking Code of Practice.

You can download a copy of the Customer Owned Banking Code of Practice from our website.

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice you can contact:

Customer Owned Banking Code Compliance Committee
PO Box 14240 Melbourne VIC 8001

**Phone.** 1800 931 678

**Email.** info@codecompliance.org.au

## 22. Privacy notice.

### 22.1. What information can be used and 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.

### 22.2. 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.

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.

### 22.3. 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 third parties.

### 22.4. 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. 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.

### 22.5. Security and privacy policy.

#### 22.5.1. 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.

#### 22.5.2. Privacy policy.

Our privacy policy (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.

### 22.6. Contact Us.

**Privacy Officer.**

Our Privacy Officer's contact details are:

**Postal Address.**
Privacy Officer
PO BOX 14537
Melbourne VIC 8001

**Phone.** 1800 033 139

**Email.** info@defencebank.com.au (marked to the attention of the Privacy Officer)

## 23. Definitions.

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

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

**Additional cardholder** means a person 16 years or older nominated by you and authorised by us to operate your linked account(s) alone.

**ADI means** an 'authorised deposit-taking institution' as that term is defined in the Banking Act 1959 (Cth).

**ATM** means automatic teller machine.

**Authorised user** means the user and any person the user has authorised to operate the account.

**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.
- visa transactions not yet debited
- uncollected P2P payments.

**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** means BPAY Pty Ltd (ABN 69 079 137 518).

**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, via internet access or any other access method as approved by us from time to time.

**BPAY Scheme** means the scheme operated by BPAY which governs the way in which we provide Osko to you.

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

**BECS Procedures** means the Bulk Electronic Clearing System Procedures as existing from time to time.

**BPAY** means 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.

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

**Business Day** means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned.

**Card** means a VISA Debit card or Digital Card (as the case may be).

**Card controls** means the control functions available for any VISA Debit card which is not expired, blocked, suspended or cancelled.

**Card details** means the information printed on the VISA Debit card, or displayed on the digital card, and includes, but is not limited to, the card number and expiry date.

**Cleared funds** means the proceeds of cheque deposits to your account once the cheque is cleared, cash deposits and direct credits.

**Closed** in relation to a PayID means a PayID which is removed from the PayID Service, and which you will no longer be able to use to make and receive Osko Payments.

**Conditions of Use** means these Product and Services Conditions of Use.

**Contactless** means transactions made by holding or tapping a VISA Debit card (which is capable of making a contactless transaction) in front of an electronic terminal without having to insert or swipe the card.

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

**Defence Bank Fees and Charges Schedule.** A document produced by us setting out applicable to products and services provided by us.

**Device** means a device given by a subscriber to a user that is used to perform a transaction. Examples include:

- ATM cards,
- debit cards and credit cards, whether physical or virtual,
- prepaid cards (including gift cards), whether physical or virtual,
- electronic toll devices,
- tokens issued by a subscriber that generate a passcode, and
- contactless devices

**Direct debit** means a "Direct Debit Request" as defined in the BECS Procedures

**Direct entry** means a direct debit or direct credit.

**Digital wallet** means an electronic device or an online service that securely stores payment information and allows for electronic transactions to be made.

**Electronic Banking** - facilities developed by Defence Bank to enable you, via 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.

**Electronic equipment** includes, but is not limited to, a computer, television, telephone and an Electronic Terminal.

**Electronic terminal** means the electronic equipment, electronic system, communications system or software controlled or provided by or on behalf of us or any third party for use with a VISA Debit card and PIN to conduct a Transaction and includes, but is not limited to, an ATM or point of sale terminal.

**Electronic transaction** means a payment, funds transfer or cash withdrawal Transaction initiated using Electronic Equipment that is not intended to be authenticated by comparing a manual signature with a specimen signature.

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

**Facility** means an arrangement through which you can perform transaction.

**Identifier** means information that a user knows but is not required to keep secret and must provide to perform a transaction. An example would be an account number.

**Linked account** means an account nominated by you that we authorise you to access using a VISA Debit card. If there is more than one accountholder and/or more than one signatory, each accountholder and each signatory must be authorised by us to operate the account alone.

**Locked** in relation to a PayID means a PayID which we have temporarily disabled in the PayID Service.

**Mandate Management Service** means the central, secure database operated by NPP Australia Limited of Payment Agreements

**Manual signature** means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet.

**Merchant** means a retailer or any other provider of goods or services.

**Migrated DDR Mandates** has the meaning given in Section 16.6.1.

**Mistaken internet payment** means a payment by a user through a 'Pay Someone' internet banking facility and processed by an authorised deposit-taking institution (ADI) through direct entry where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:

- the user's error, or
- the user being advised of the wrong BSB number and/or identifier.

This does not include payments made using BPAY.

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

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

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

**NPP Payments** means electronic payments cleared and settled by participating financial institutions via the NPP

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

**One time password** a secure second password is required to, amongst others, access to funds, change your daily limits, address details and apply for products delivered either through secure SMS, or for Defence Personnel the added option of receiving the one time password through a second factor authentication email to your Defence Services email address.

**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 term** 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).

**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.

**Organisational payer** means a payer who is any of the following:

- an individual acting in their capacity as a trustee, sole trade or partner of a partnership a body corporate in its personal capacity or as a trustee.
- a government agency.
- an unincorporated body or association or a firm or partnership.

**Passcode** means a password or code that the user must keep secret that may be required to authenticate a transaction or user. A passcode may consist of numbers, letters, a combination of both, or a phrase. Examples include:

- personal identification number (PIN),
- internet banking password,
- telephone banking password,
- code generated by a physical security token, and
- code provided to a user by SMS, email or in a mobile application.

* A passcode does not include a number printed on a device (e.g. a security number printed on a credit or debit card).

**Pay Someone banking facility** means a facility where a user can make a payment from one bank account to a third party's bank account by entering, selecting or using a Bank/State/Branch (BSB) and account number, PayID or other identifier, but does not include BPAY or PayTo payments.

**Payment Agreement** means an agreement established by you and an approved merchant or Payment Initiator, by which you authorise us to make payments from your account. Other than in Section 16.1 "Creating a PayTo Payment Agreement", it includes a Migrated DDR Mandate.

**Payment Initiator** means an approved payment service provider who, whether acting on behalf of you or a merchant, is authorised by you to initiate payments from your account.

**PayTo** means the service which enables us to process NPP Payments from your account in accordance with and on the terms set out in a Payment Agreement you have established with a merchant or Payment Initiator that subscribes to the service.

**Receiving ADI** means an authorised deposit-taking institution whose customer has received an internet payment.

**Recurring Payment Authority** means either a recurring or an instalment payment agreement between you (the cardholder) and a Merchant in which you have preauthorised the Merchant to bill your account at predetermined intervals (eg. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.

**Round Up** is a phrase used to describe an optional feature on selected transaction and offset accounts that works by debiting the round up amount from one account and crediting it into a secondary account, usually a savings account.

**Round Up amount** means the difference between the purchase amount of an eligible transaction made with a VISA Debit card (including the information printed on it or a Digital Card) and the nearest $1 (rounded up).

**Service provider** in relation to Osko means a person engaged by BPAY to provide goods or services to BPAY in connection with Osko.

**Terms and Conditions** means these Product and Services Terms and Conditions.

**Transaction** means a transaction to which the ePayments Code applies or which was processed through the new payments platform operated by NPP Australia Limited.

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

**Transfer ID** means a unique identification number generated by the Mandate Management Service in connection with a request to transfer one or more Payment Agreements

**Unauthorised Transaction** means a transaction that is not authorised by a user. It does not include any transaction that is performed by a user themselves or by anyone who performs a transaction with the knowledge and consent of a user.

**Uncleared funds** means when the proceeds of deposits (cheques, direct credit and cash) has not cleared into your account.

**Unintended recipient** means the recipient of funds as a result of a mistaken internet payment

- when you report a mistaken internet payment, we must investigate whether a mistaken internet payment has occurred
- if we are satisfied that a mistaken internet payment has occurred, we must send the receiving ADI a request for the return of the funds.

**User** means you or an individual you have authorised to perform transactions on your account, including: a third party signatory to your account and a person you authorise us to issue an additional card to.

**VIP access** A level two security feature you may register to use as provided by Symantec™ Validation and 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.

**We** and **us** means Defence Bank (ABN 57 087 651 385).

**You** and **your** means the person or persons in whose name an account and access facility is held.

# We’re here to help.

## It’s easy and convenient to contact us.

**Here’s how:**

- 1800 033 139
- visit your local Defence Bank branch
- defencebank.com.au
- info@defencebank.com.au

Defence Bank Limited ABN 57 087 651 385
AFSL/Australian Credit Licence 234582.
Head Office, Level 10, 31 Queen Street, Melbourne VIC 3000.

B025 (24/10/2024)