ANZ ONLINE
ADMINISTRATOR GUIDE

ANZ

TABLE OF CONTENTS

INTRODUCTION TO ANZ ONLINE

ABOUT THIS GUIDE

This document covers essential processes and procedures for ANZ Online Administrators. It is recommended that Administrator Users read this guide in conjunction with the ANZ Online Terms and Conditions.

LEARNING ABOUT ANZ ONLINE

The following range of resources are available to assist you in your use of ANZ Online.

1. ANZ ONLINE HELP

The online help should be your primary source of information about using ANZ Online.

As new operating features or functions, particularly those relating to security, integrity and authentication are introduced, instructions covering changes and the usage of such features will be provided.
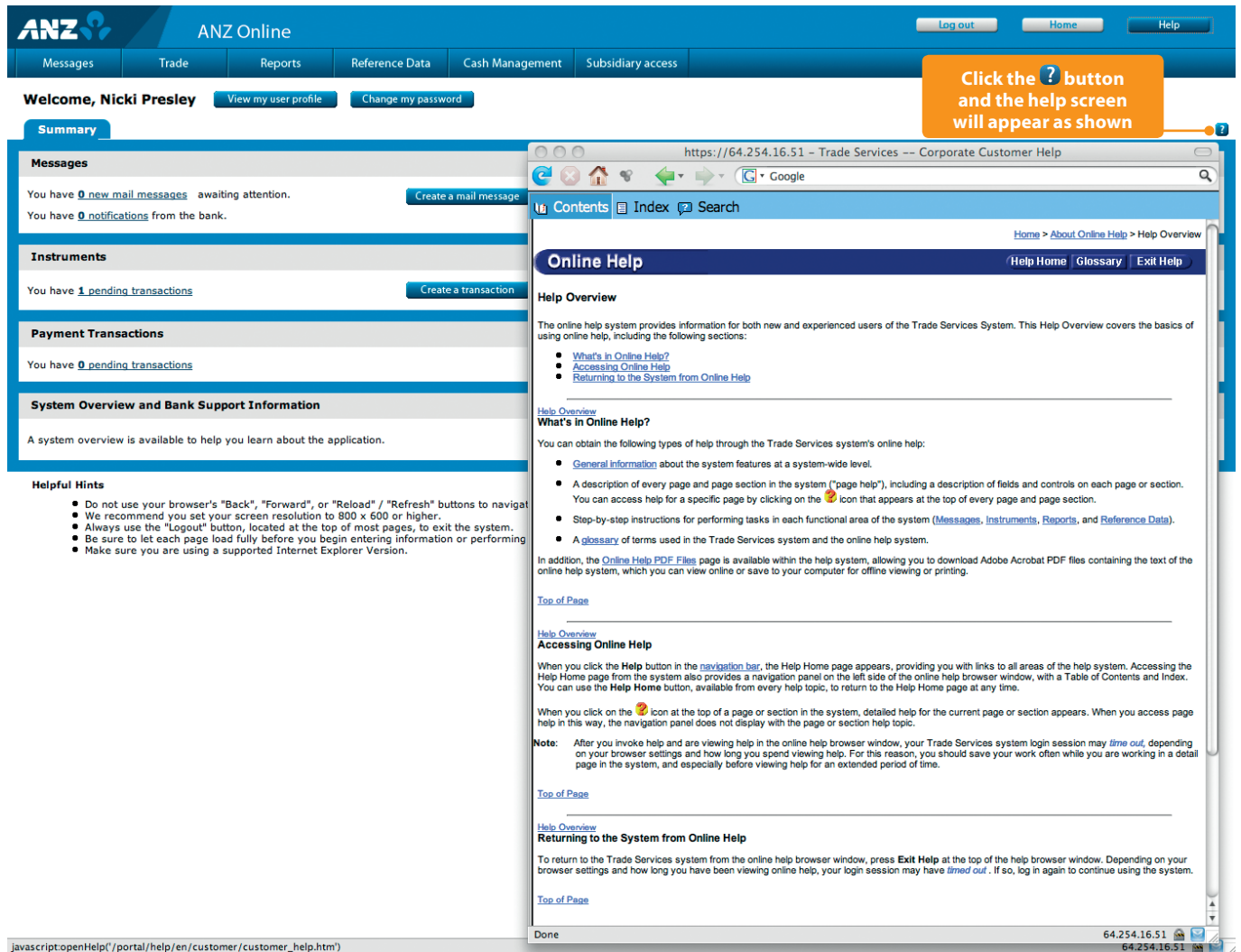
As shown below, there are two ways to access ANZ Online help.

1. The Help button at the top of the page provides a complete online help index for the majority of ANZ Online functions.

Click the 'Help' button and the help screen will appear as shown

INTRODUCTION TO ANZ ONLINE

2. The ? button provides a help function for the specific page you are accessing.

2. GENERAL SYSTEM NAVIGATION INFORMATION

To navigate through ANZ Online simply use the page controls available within the system. It is recommended you do not use the controls on your browser's toolbar (such as Back, Forward and Refresh) to navigate through the system.

General system navigation information is also provided within the ANZ Online online help. See the Navigating the System section of the ANZ Online help.

3. SUPPORT INFORMATION

When you first log on to ANZ Online, your home page appears. To view ANZ contact numbers and updates about the system, click the View Support Information button.

MINIMUM SPECIFICATIONS

Below is the list of specifications required to access ANZ Online.

OPERATING SYSTEM

The following five operating systems are supported:

> Windows Microsoft 7

> Windows Microsoft Vista

> Windows Microsoft XP

> Windows Microsoft 2000

> Windows Microsoft NT

Macintosh is currently not supported for any User.

FIREWALL AND ANTIVIRUS SETTINGS

Please ensure the appropriate permissions are configured for both firewall and antivirus software to allow Users to access ANZ Online.

OPERATING SYSTEM AND BROWSER VERSION

Below is the summary of compatible operating systems and browser versions for Token Users.

BROWSER TYPE & VERSION	JAVA VIRTUAL MACHINE (JVM)	WINDOWS 7	WINDOWS VISTA	WINDOWS XP PROFESSIONAL SP1/SP2/SP3	WINDOWS 2000	WINDOWS NT
Microsoft Internet Explorer 6.0 (SP1 & SP2)	MS 5.00.3802 SUN 1.4.2.0	Supported	Supported	Supported	Supported	Supported
Microsoft Internet Explorer 7.0	MS 5.00.3802 SUN 1.4.2.0 SUN 1.5.2.0	Supported	Supported	Supported	Supported	Supported
Microsoft Internet Explorer 8.0	MS 5.00.3802 SUN 1.4.2.0 SUN 1.5.2.0	Supported	Supported	Supported	Supported	Supported

Below is the summary of compatible operating systems and browser versions for Smartcard Users.

BROWSER TYPE & VERSION	JAVA VIRTUAL MACHINE (JVM)	WINDOWS XP PROFESSIONAL SP1/SP2/SP3	WINDOWS VISTA	WINDOWS 7
Microsoft Internet Explorer 7.0 & 8.0	MS 5.00.3802 SUN 1.4.2.0	Supported	Supported	Supported
Microsoft Internet Explorer 6.0	-	Supported	-	-

Macintosh is currently not supported by any user.

INTERNET CONNECTION

An internet speed of 56kbps or higher is recommended.

VIDEO RESOLUTION

A minimum screen resolution of 800 x 600 is recommended.

HARDWARE REQUIREMENTS

Token Users and User ID/password Users:

> Token (provided by ANZ)

> No software installation required.

Smartcard Users:

> CD-ROM drive for software installation (or access over a network)

> Available and enabled USB port required.

ANZ ONLINE SECURITY INFORMATION

The following security is in place to protect your organisation when using ANZ Online.

INTRODUCTION TO ANZ ONLINE

PHYSICAL SECURITY

All buildings that contain ANZ Online web servers and/or database servers use industry-standard physical security to prevent access by unauthorised people.

DATA ENCRYPTION

All data communication to and from ANZ Online uses 128-bit Secure Sockets Layer encryption and HTTPS (Hypertext Transfer Protocol – Secure) as communication protocol.

FIREWALLS

Firewalls protect all data used in ANZ Online. Firewalls assist to ensure that data is only provided in response to valid requests from the application. It is advisable for your organisation to also have a firewall to protect its own computers and networks.

It is recommended that antivirus and anti-spyware software are installed on computers, particularly when linked to a broadband connection, digital subscriber line or cable modem. It is recommended to update anti-virus and firewall products with security patches or new versions on a regular basis.

AUTHENTICATION

ANZ Online will verify the identity of each User accessing ANZ Online by the following three authentication methods:

> A User ID and password

> A Token device OR

> A Smartcard

To authenticate a User the following action is taken:

> The type of User is identified and the User's identity is verified

> Confirm the User is permitted access to ANZ Online

Once authenticated the User's functionality is controlled by the assigned security profile, which is discussed in the Security Profiles section.

SECURITY PROFILES

An Administrator can assign a security profile for all Users on ANZ Online that do not require a security device.

> A security profile determines which module of ANZ Online Users can access

> The functions Users can use within each module of ANZ Online

THRESHOLD GROUPS

If your use of ANZ Online involves authorising cash payment and/or trade transactions, then your organisation's Administrator may have assigned you a threshold group.

Your threshold group determines the value of transactions that you can authorise. For each type of transaction, there are limits for the:

> Threshold amount, which is the largest single transaction you can authorise

> Daily maximum value of the transactions you can authorise

PANEL AUTHORITY

If your use of ANZ Online involves authorising cash payment transactions, then your organisation's Administrator may have assigned you a panel authority.

Your panel authority determines the amount range of the transactions that you can authorise and your panel User group.
For each type of transaction under panel authorisation, there is an amount range assigned to each authoriser. This will determine how many panel authorisers from different panel groups are required to authenticate a transaction.

SEGREGATION OF DUTIES

ANZ Online allows your organisation to enforce segregation of duties between employees, which provides an additional form of security. For example:

> Transactions may need to be authorised by someone other than the last person who entered data for those transactions

> Transactions may require multiple authorisations. (e.g. via a panel authorisation or by users from different work groups)

REPORTING CATEGORIES

> ANZ Online allows the ability to assign users to reports based on their roles and responsibilities within your organisation. Four report categories (Cash Payments, Trade Services, Confidential and Administrator) will be available to users and can be assigned to users via their user profile page. Only reports within that selected category will be available to the user from the Reports navigational tab. User's can have up to all four categories assigned to them.

PROTECTING YOUR BANKING

> Users should check the authenticity of the financial institution's website prior to accessing available products and services

> Users should verify when accessing products and services offered by the financial institution that the browser session is secure. This can be verified by ensuring the webpage begins with "https://" rather than "http://", and the security lock is displayed on the bottom right of the browser. Users should not commence transactions prior to verifying

> Always log out of ANZ Online by using the log out button in the top right hand corner of the browser

> Do not install software or run programs of unknown origin

> Delete junk or chain emails

> Do not open email attachments from unknown senders

> Do not disclose personal, financial or credit card information to suspect websites or unknown recipients

> Do not use a computer or a device which cannot be trusted

> Do not use public or internet café computers to access banking products and services

> Do not share resources from your computer, (i.e. hard drives and printers) whilst operating on the internet

> Do not disclose your password or security device passphrase to anyone else

> If your security device is lost or stolen you must notify the ANZ Online Support Centre immediately to have the security device suspended or revoked

GENERAL SYSTEM TASKS

This section outlines general system tasks for ANZ Online. The following tips will assist you in your use of ANZ Online.

SESSION TIMEOUTS AND SAVING YOUR WORK

When using ANZ Online, your session will time out after 15 minutes of inactivity. A pop-up window will appear two minutes prior to session timeout, advising you that you have two minutes left before the session is timed out. When your session times out:

> The system will save any work you have done on the Transaction and Reference Data pages, providing the entry meets the validation criteria

> The time out page will display any errors encountered in attempting to validate and save the information

It is recommended that the User should save work periodically while working in ANZ Online.
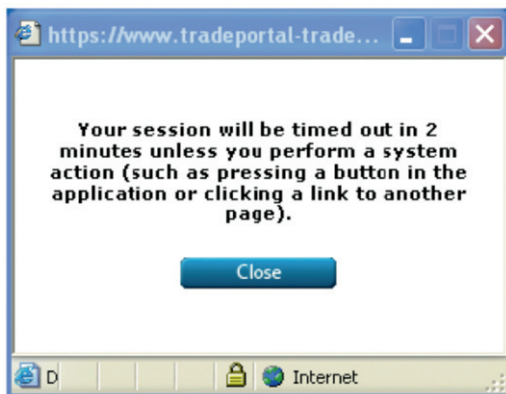
GENERAL SYSTEM TASKS

LOGGING OUT

When you've finished using ANZ Online, **it is important to log out properly** rather than simply closing the application window.

If you close the window rather than using the Log out button, ANZ Online considers you to be still logged in. This means you cannot log in again until your current session times out (approximately after 15 minutes).

Please ensure you click the 'Log Out' button to exit the session in a secure manner.

Log off the online session and turn off the computer when not in use.

GENERAL SYSTEM TASKS

VIEWING YOUR USER PROFILE

WHAT IS A USER PROFILE?

Your User profile contains details stored about you in ANZ Online. In particular, it contains:

> Personal details, such as your name and address

> Details of the security profile and threshold group that has been assigned to you (see Security profiles and Threshold groups)

HOW TO VIEW YOUR USER PROFILE

To view your User profile, complete the following steps:

STEP	ACTION
1	If your ANZ Online **Home** page is not displayed, click the **HOME** navigation button to display it.
2	Click the **View My User Profile** button. Your User profile appears.
3	When you've finished viewing your User profile, click the **Close** button.

CHANGING YOUR USER PROFILE

Users are unable to change their own profiles. For modifications to their profiles, users can contact their company Administrator for restricted changes or contact the bank for assistance.

GENERAL SYSTEMS TASKS

TRANSLATIONS

Language content within ANZ Online can be customised to suit organisation Users. The following range of User languages are available:

> Traditional Chinese

> Vietnamese

> Simplified Chinese

> Korean

> Japanese

The following categories of translated content are available:

> Labels

> Buttons

> Error messages

> Warning and information messages

ASSIGNING USER LANGUAGE

Simply follow the steps below to assign the language option for each of your users:

STEP	ACTION
1	Log on to ANZ Online
2	Select the **REFERENCE DATA** tab
3	Select **Users** from the drop-down list.

GENERAL SYSTEMS TASKS

STEP	ACTION
4	Select the User profile that you want to change the language settings for from the list displayed
5	Go to the **REGIONAL SETTINGS** drop down box and select the language you wish to assign to the User
6	Click the **SAVE & CLOSE** button
7	Request the user to log into ANZ Online to now view the regional settings in the selected language

UNICODE FUNCTIONALITY

Unicode functionality is available for specific input data fields required for Domestic Payments in some countries.
Please refer to the ANZ Online File Format Guides for further details and clarification on the Unicode fields available.

> Unicode functionality is not available for any other Payment functionality or Direct Debits apart from Domestic Payments.

> Unicode functionality is not available for payment amounts, dates and accounts.

MANAGING USERS

As an ANZ Online Administrator you are able to complete a range of activities in relation to ANZ Online Users within your organisation. This section outlines those activities.

CREATE A USER ID / PASSWORD USER

Follow these steps to set up a new non-security device User.

BEFORE YOU BEGIN

Before you can add a User to ANZ Online, make sure you have:

> the personal details of the User that you want to create, and

> details of the ANZ Online security profile and threshold group required for the new User

If your organisation requires Users to be issued with either Smartcards or Tokens to access ANZ Online, your company must complete an application form with the required user details and authorised signatures and submit to ANZ for processing.

Note: All company authorisers and administrators require a security device to access ANZ Online.

CREATING A USER ID / PASSWORD IN ANZ ONLINE

To create a User ID / password User complete the following steps:

STEP	ACTION
1	Log on to ANZ Online, if you are not already logged in
2	Click the **REFERENCE DATA** navigation button The **Reference Data** page appears
3	From the **Show** list, select **Users** A list of your organisation's Users appears
4	Click the **Create a User** button The **User** page appears
5	Create a unique **User ID** for the User as per the below suggested naming conventions: > Whole ID must be in uppercase > Maximum 10 characters > The ID must comprise of: Surname first (1st 6 letters only), then the initial of the user's first name, followed by first three letters of company ID, e.g. David Wong from ABC Book Shop would be WONGDAB C
6	Enter **User** information into the page by completing all mandatory fields For information about what data is required in particular fields, click the 🛈 button for assistance
7	In the **Security** section, ensure the radio button is selected for the user to enter a **Login ID** and **Password** for authentication
8	Enter the User's unique **User ID** as created in Step 5 into the **Login ID** field This is the **Login ID** the user will use to access ANZ Online
9	Enter a temporary password into the **New Password** and **Retype New Password** fields See **Password Rules** for creating and/or resetting a user's password in ANZ Online
10	Select the user's **Security Profile** which will determine the user's rights within ANZ Online
11	Select the account numbers and/or report categories for the user to have access to
12	Select the **Save & Close** button when completed

MANAGING USERS

PASSWORD RULES

The following password recommendations can be used when creating a password for a User ID/password.

PASSWORDS MUST	PASSWORDS MUST NOT
Contain at least 8 characters but no more than 30 characters	Contain three consecutive characters that are the same
	Start or end with a space character
Contain both upper- and lower-case letters	Be the same as your User ID, First Name, Last Name, or Login ID, regardless of case
Contain at least one number (0…9)	Be the same as any of your last 13 passwords
	Contain three consecutive characters that are the same
	Consist of repeating characters (i.e. aaaaaaaa)
	Consist of sequential numbers or letters

> Passwords are case sensitive (for example, xyz0123 is different to XyZ0123)

> Passwords will expire every 90 days

> After three failed login attempts, the user will be logged out and their password will be required to be reset by the company administrator.

> After ten failed login attempts, the user will be locked out and their password will be required to be reset by the bank. This count is cumulative and is not reset after you successfully log in. However, the count is reset when a password is changed

> ANZ Online passwords should not be used for different websites, applications or services, particularly when they relate to different entities

> Users should not select the browser option for storing or retaining User names and passwords

MANAGING USERS

RESETTING A USER'S PASSWORD

Follow these steps to reset a User password.

USER ID / PASSWORD USERS

To reset a User's password, complete the following steps:

STEP	ACTION
1	Log on to ANZ Online, if you are not already logged in
2	Click the **REFERENCE DATA** navigation button The **Reference Data** page appears
3	From the **Show** list, select **Users** A list of your organisation's Users appears
4	Select the user from the list to reset their password
5	In the **Security** section of the User page, type the User's new temporary password in the New Password and Retype New Password boxes Note: Passwords must comply with the password rules
6	Click the **Save & Close** button The User's details are saved
7	Inform the **User** of their new temporary password. The User will be prompted to change their password the next time they log on

TOKEN USER

If your ANZ Online access is suspended, please contact the ANZ Online Support Centre to have your Token reinstated.

SMARTCARD USER

If your ANZ Online Smartcard PIN has been disabled, the user will be required to request another Smartcard via an application form and submit to the bank. The PIN cannot be reset as all information is sorted on the microchip on the card.

MANAGING USERS

MAINTAINING USER DETAILS

DISPLAYING A USER'S ANZ ONLINE DETAILS

There are a number of procedures where the first step is to display the User's details on the **User** page in ANZ Online.
To do this, complete the following steps:

STEP	ACTION
1	Log on to ANZ Online
2	Click the **REFERENCE DATA** navigation button The **Reference Data** page appears
3	From the **Show** list, select **Users** A list of your organisation's Users appears
4	In the **User ID** column, click the name of the User details you want to display The **User** page appears

CHANGING A USER'S NAME, ADDRESS OR OTHER GENERAL DETAILS

To change a User's name or other general details, complete the following steps:

STEP	ACTION
1	Display the User's details For instructions, see Displaying a User's ANZ Online details
2	Change the User's details as required For information about the data required in particular fields, click the button for the relevant section of the page
3	When you have finished entering data, click the **Save & Close** button to save the User's details

SUSPEND / RE-INSTATE USER ACCESS

Security device Users can be temporarily suspended from accessing ANZ Online. Please contact the ANZ Online Support Centre for assistance.

DELETING SECURITY DEVICE USERS

Please contact the ANZ Online Support Centre to delete / unassign Security Device Users from your organisation.

DELETING NON-SECURITY DEVICE USERS

Company administrators can delete a user profile that does not maintain a security device. To do this, complete the following steps:

STEP	ACTION
1	Log into ANZ Online
2	Click on **Reference Data** navigation button
3	From the **Show** list, select **Users**
4	Select the **User ID** that is to be deleted
5	From the user profile page, select the **Delete** button
6	A message to confirm deletion will be presented. Select **OK** to complete the deletion process. User will now be deleted from the list

MANAGING REFERENCE DATA

This section outlines the reference data available in ANZ Online.

TYPES OF REFERENCE DATA

Reference data is information that is either:

> required by the system (e.g. security profiles, Users, threshold groups, panel groups and template groups)

> used to create transactions (e.g. templates, parties, phrases)

When registering for ANZ Online, your organisation will specify a number of default system settings that will govern the organisation's requirements. These settings provide the base set of reference data for the organisation.

Permissions to create and maintain reference data are usually provided to a small number of Users only.
For example:

> an administrator might manage system-related reference data such as security profiles, threshold groups, panel groups and Users

> a financial controller might manage payment reference data such as templates and phrases

SECURITY PROFILES

A security profile is a group of system permissions that can be assigned to one or more ANZ Online Users.
The permissions assigned determine what each User can create, view, edit, authorise or delete within ANZ Online.

For example, some Users might be able to view transactions, while others can create and authorise them.

The security profile assigned to a User depends on their role within your organisation. It is your responsibility to:

> define appropriate security profiles for your organisation

> assign the correct profile to each User

Note: Any security profile changes to a user's profile that requires or maintains a security device can impact the user's ability to perform their related functions within ANZ Online

INITIATOR USERS

Users assigned with an Initiator security profile will automatically be assigned the ability to upload payment files by default.

THRESHOLD GROUPS

A threshold group defines authorisation limits for Users in relation to:

> the largest individual transactions they can authorise

> the combined maximum value of the transactions they can authorise each day

A threshold group can have different transaction and daily limits for each instrument and transaction type.

The threshold group assigned to a User depends on their role within your organisation. It is your responsibility to:

> define appropriate threshold groups for your organisation

> assign the correct threshold group to each User

Note: The use of threshold groups is optional. There is also the option of setting up panel authorities. To set up a panel authority you will need to contact the ANZ Online Support Centre. It's important to understand that if a threshold group is not assigned, the User will be able to authorise an unlimited value of transactions.

USERS

Each User has a unique User profile, which contains:

> general information about the User, such as name and contact information

> security access settings relating to passwords, Smartcards or Tokens

> details of the threshold group and security profiles assigned to the User

> details of the template groups, account numbers and reporting categories assigned to the User

> details if the Confidential Payment Indicator is selected. If selected, the User will have access to confidential payments and transaction templates created. The ability to initiate new payment transactions from templates that have been selected as confidential will also be possible.

PARTIES

A user can store commonly used Beneficiary party information in ANZ Online such as the party name, address, account numbers, etc. After you create a party in the Reference Data tab, the party details can be retrieved from any transaction when the Search for a Beneficiary button is selected. Once the required party has been selected from the list, the beneficiary details will auto-populate into the transaction.

PHRASES

A user can store commonly used phrases that contains a standard text statement for insertion into a specific field within a transaction. Examples of phrases include:

> settlement instructions or standard goods descriptions

Note: Phrases can then be edited once selected within a transaction

TEMPLATE GROUPS

> Provides the ability to assign templates to a group and to define which Users can use which groups. Enables further control over the type of Instruments a User can create.

INSTRUMENT TEMPLATES

An instrument template is a predefined set of commonly used details within a single transaction. This allows the user to select a template when creating a new transaction whereby most of the required fields have already been input. Minimum details will be required to be entered or edited before Verifying the transaction.

An Instrument template can be assigned to a Template Group, and can have a Confidential Payment Indicator assigned, and can also be a fixed template.

FIXED TEMPLATE

> A fixed template is one in which the data fields can not be edited.

> Is only available for Cash payments eg: BKT, BCHK, ACH/GIRO, CBFT.

FOREIGN EXCHANGE RATES

Foreign exchange rates are indicative rates required for transaction authorisation purposes. ANZ Online uses available rates to convert transaction amounts to your organisation's base currency in order to correctly calculate the user's threshold limits.

MANAGING REFERENCE DATA

Follow these steps to manage your reference data. You can view, create, edit and delete reference data in ANZ Online.

For further information, see the following section of the ANZ Online help:
Using the System > Reference Data Procedures.

CREATING REFERENCE DATA

Note: You cannot edit or delete any reference data that was 'Added by' the bank

To create reference data, complete the following steps:

STEP	ACTION
1	Log on to ANZ Online
2	Click the **REFERENCE DATA** navigation button
	The **Reference Data** page appears
3	From the **Show** list, select the type of reference data you want to create, view, edit or delete
	A table appears, listing the existing reference data items of the selected type
	If your security profile allows you to create reference data, a **Create button** also appears. For example, if you selected **Parties** from the **Show** list, the button is labelled **Create a Party**
4	Click the **Create a reference data item** button
	The relevant reference data creation page appears
5	Enter the details required for the reference data item into the page
	For information on what data is required in particular fields, click the button for the relevant section of the page
6	When you have finished entering the details of the reference data, click the **Save & Close** button to save the reference data item

MANAGING REFERENCE DATA

DISPLAYING A REFERENCE DATA ITEM

To display a particular reference data item, complete the following steps:

STEP	ACTION
1	Log on to ANZ Online
2	Click the **REFERENCE DATA** navigation button The **Reference Data** page appears
3	From the **Show** list, select the type of reference data item you want to view A table appears, listing the existing reference data items of the selected type
4	Click the reference data item you want to view The item you selected is displayed

CHANGING REFERENCE DATA

To change a reference data item, complete the following steps:

STEP	ACTION
1	Display the reference data item you want to change For instructions, see Displaying a reference data item
2	Change the reference data item as required For information regarding data required in particular fields, click the button for the relevant section of the page
3	When you have finished changing the reference data item, click the **Save & Close** button

DELETING REFERENCE DATA

NOTE: You cannot edit or delete any reference data that was 'Added by' the bank

To delete a reference data item, complete the following steps:

STEP	ACTION
1	Display the reference data item you want to change For instructions, see Displaying a reference data item
2	Click the **Delete** button A message appears asking you to confirm the deletion of the item
3	Click the **OK** button The item is deleted

ANZ