Privacy Policy

Financial Force Pty Ltd

Company:	Financial Force Pty Ltd
AFSL:	238337
Version Number:	Version 3
Date Updated:	31/10/2026

TABLE OF CONTENTS

SECTION A – INTRODUCTION 5

1. INTRODUCTION 5

2. WHEN DOES THIS POLICY APPLY? 5

3. GLOSSARY 5

SECTION B – CONSIDERATION OF PERSONAL INFORMATION PRIVACY 7

4. PRIVACY STATEMENT 7

SECTION C – COLLECTION OF PERSONAL INFORMATION (SOLICITED PERSONAL INFORMATION) 8

5. PERSONAL INFORMATION (OTHER THAN SENSITIVE INFORMATION) 8

6. SENSITIVE INFORMATION 8

7. MEANS OF COLLECTION 10

8. INFORMATION COLLECTED BY FINANCIAL FORCE 9

9. PURPOSE OF COLLECTION 9

SECTION D – COLLECTION OF PERSONAL INFORMATION (UNSOLICITED PERSONAL INFORMATION) 11

10. DEALING WITH UNSOLICITED PERSONAL INFORMATION 10

SECTION E – NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION 10

11. NOTIFICATION OF COLLECTION 10

SECTION F – USE OR DISCLOSURE OF PERSONAL INFORMATION 13

12. USE OR DISCLOSURE 13

13. WHO DOES FINANCIAL FORCE DISLCOSE PERSONAL INFORMATION TO? 13

SECTION G – DIRECT MARKETING 16

14. DIRECT MARKETING 16

15. EXCEPTION – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION . 16

16. EXCEPTION – SENSITIVE INFORMATION 16

17. REQUESTS TO STOP DIRECT MARKETING 16

SECTION H – CROSS BORDER DISCLOSURE OF PERSONAL INFORMATION 18

18. DISCLOSING PERSONAL INFORMATION TO CROSS BORDER RECIPIENTS 18

SECTION I – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT IDENTIFIERS..... 19

19. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS 19

20. USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS 19

SECTION J – INTEGRITY OF PERSONAL INFORMATION..... 20

21. QUALITY OF PERSONAL INFORMATION..... 20

22. SECURITY OF PERSONAL INFORMATION 20

23. STORAGE OF PERSONAL INFORMATION..... 20

SECTION K – ACCESS TO, AND CORRECTION OF, PESRONAL INFORMATION 21

24. ACCESS..... 21

25. EXCEPTIONS..... 21

26. REFUSAL TO GIVE ACCESS..... 21

SECTION L – CORRECTION OF PERSONAL INFORMATION..... 23

27. CORRECTION OF INFORMATION..... 23

28. REFUSAL TO CORRECT INFORMATION..... 23

29. REQUEST FROM A CLIENT TO ASSOCIATE A STATEMENT WITH THEIR INFORMATION 23

30. DEALING WITH REQUESTS..... 23

SECTION M – MAKING A PRIVACY COMPLAINT 25

31. COMPLAINTS..... 26

SECTION N – MISCELLANEOUS..... 20

32. NOTIFIABLE DATA BREACHES SCHEME..... 20

33. POLICY BREACHES 20

34. RETENTION OF FORMS 21

35. POLICY REVIEW 21

VERSION CONTROL

Version Number	Date Updated/Reviewed	Notes
1	28/10/2021	Original document prepared and finalised.
	31/10/2022	Reviewed
	31/10/2023	Reviewed
	31/10/2024	Reviewed
2	31/10/2025	Updated
3	28/02/2026	Updated - Added AML/CTF Legislation related sections

SECTION A – INTRODUCTION

1. INTRODUCTION

1.1 As part of Financial Force Pty Ltd's ("**Financial Force**") process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, Financial Force has adopted this Privacy Policy ("**Policy**") to manage personal information in an open and transparent manner.

1.2 The provisions of this Policy will assist Financial Force in complying with the requirements of the *Privacy Act 1988* (Cth) ("**Privacy Act**") and the Australian Privacy Principles in protecting the personal information Financial Force holds about its clients.

1.3 This Policy applies to all Corporate Authorised Representatives, Authorised Representatives and Sub-Authorised Representatives of Financial Force.

2. WHEN DOES THIS POLICY APPLY?

2.1 This Policy applies to all representatives and employees of Financial Force at all times and the requirements remain in force on an ongoing basis.

3. GLOSSARY

TERM	DEFINITION
AML/CTF Legislation	means: (a) *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*; and Anti-Money Laundering and Counter-Terrorism Financing Rules 2025.
APP entity	means an agency or organisation as defined in section 6 of the Privacy Act.
Australian law	means (a) an Act of the Commonwealth or of a State or Territory; or (b) regulations, or any other instrument, made under such an Act; or (c) a Norfolk Island enactment; or (d) a rule of common law or equity.
Collects	Financial Force collects personal information only if Financial Force collects the personal information for inclusion in a record or generally available publication.
Court/tribunal order	means an order, direction or other instrument made by: (a) a court; or (b) a tribunal; or (c) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or

	(d) a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or (e) a member or an officer of a tribunal; and includes an order, direction or other instrument that is of an interim or interlocutory nature.
Credit Reporting Body	means: (a) an organisation; or (b) an agency prescribed by the Privacy Regulations; that carries on a credit reporting business.
De-identified	personal information is *de-identified* if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
Eligible Data Breach	An eligible data breach occurs: (a) where there has been unauthorised access of unauthorised disclosure of personal information, or a loss of personal information, that Financial Force holds; and (b) the unauthorised access or unauthorised disclosure is likely to result in serious harm to one or more clients; and (c) Financial Force is not able to prevent the likely risk of serious harm with remedial action.
Holds	Financial Force *holds* personal information if it has possession or control of a record that contains the personal information.
Identifier of an individual	means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include: (a) the individual's name; or (b) the individual's ABN (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*); or (c) anything else prescribed by the regulations.
Permitted general situation	As defined in s16A of the Privacy Act
Permitted health situation	As defined in s16B of the Privacy Act
Personal information means	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

Sensitive information	means (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information. (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

SECTION B – CONSIDERATION OF PERSONAL INFORMATION PRIVACY

4. PRIVACY STATEMENT

4.1 Financial Force's Director must ensure that at all times the provisions of this policy are implemented in the day to day running of Financial Force.

4.2 Director must ensure that at all times this Policy:

(a) is current and reflects the latest applicable Australian laws; and

(b) contains the following information:

(i) the kinds of personal information that Financial Force collects and holds;

(ii) how Financial Force collects and holds personal information;

(iii) the purposes for which Financial Force collects, holds, uses and discloses personal information;

(iv) how an individual may complain about a breach of the Australian Privacy Principles, or other relevant legislation that binds Financial Force, and how Financial Force will deal with such a complaint;

(v) whether Financial Force is likely to disclose personal information to overseas recipients;

(vi) if Financial Force is likely to disclose personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in this policy.

4.3 Financial Force must ensure that the Financial Force's Privacy Statement is available free of charge and in such form as appropriate. Financial Force will make the Privacy Statement available on its website.

4.4 If the Privacy Statement is requested in a particular form, Financial Force will take such steps as are reasonable to provide the Privacy Statement in the form requested.

SECTION C – COLLECTION OF PERSONAL INFORMATION (SOLICITED PERSONAL INFORMATION)

5. PERSONAL INFORMATION (OTHER THAN SENSITIVE INFORMATION)

5.1 This Section C applies to the collection of personal information that is solicited by Financial Force.

5.2 Financial Force must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of Financial Force's functions or activities.

5.3 Financial Force's may collect your personal information on an ongoing basis. It may be collected via an application form, telephone, fax or e-mail from you or another party such as a financial planner, accountant, fund manager or other source.

Our website may collect general information of a statistical nature including the number of visitors visiting the site, the time, duration and pages visited. This helps us to understand the priorities of our users so that we can improve the service, products and information we offer. General information is also collected by us on an ongoing basis from other sources as a result of our information requirements for the services we offer.

To do this, we may need to collect the following types of personal information:

- details to ascertain your financial objectives and needs
- details to determine you risk profile and investment preferences;
- details of your current financial circumstances including assets and liabilities, income and expenditures etc
- details about your employment history, family structure (i.e. dependents and spouses), commitments and social security eligibility;
- details about your current health and medical history where relevant for risk insurance purposes.

The personal details we request are used only for providing services to you. They will not be passed on to third parties other than in the performance of the service clients have engaged us to perform. We will not publish, sell, trade, loan, rent, disclose or re-use the information you give us without your express consent.

6. SENSITIVE INFORMATION

6.1 Financial Force must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and the information is reasonably necessary for one or more of Financial Force's functions or activities (as described in section 5.3); or

(b) the collection of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

(c) a permitted general situation exists in relation to the collection of the information by Financial Force; or

(d) a permitted health situation exists in relation to the collection of the information by Financial Force.

7. MEANS OF COLLECTION

7.1 Financial Force must only collect personal information by lawful and fair means.

7.2 Financial Force must only collect personal information about an individual from the individual (rather than someone else), unless it is unreasonable or impracticable to do so or the individual has instructed Financial Force to liaise with someone else.

7.3 Financial Force will collect personal information from an individual when:

(a) Financial Force's Application Form is completed;

(b) a Client provides the information to Financial Force's authorised representatives face to face, over the telephone or via email;

(c) a Client provides the information to Financial Force on the website;

(d) Financial Force/Financial Force's authorised representatives needs clients' consent to share the information to external service provider

8. INFORMATION COLLECTED BY FINANCIAL FORCE

8.1 The information Financial Force collects may include the following:

(a) name;

(b) date of birth;

(c) postal or email address; or

(d) phone numbers;

(e) other information Financial Force considers necessary to their functions and activities.

9. PURPOSE OF COLLECTION

9.1 If an individual is acquiring or has acquired a product or service from Financial Force, the individual's personal information will be collected and held for the purposes of:

(a) checking whether an individual is eligible for Financial Force's product or service;

(b) providing the individual with Financial Force's product or service;

(c) managing and administering Financial Force's product or service;

(d) protecting against fraud, crime or other activity which may cause harm in relation to Financial Force's products or services;

(e) complying with legislative and regulatory requirements in any jurisdiction;

(f) to assist Financial Force in the running of its business;

9.2 Financial Force may also collect personal information for the purposes of letting an individual know about products or services that might better serve their needs or other opportunities in which they may be interested. Please refer to Section G for further information.

SECTION D – COLLECTION OF PERSONAL INFORMATION (UNSOLICITED PERSONAL INFORMATION)

10. DEALING WITH UNSOLICITED PERSONAL INFORMATION

10.1 If Financial Force:

(a) receives personal information about an individual; and

(b) the information is not solicited by Financial Force

Financial Force must, within a reasonable period after receiving the information, determine whether or not it was permitted to collect the information under Section C above.

10.2 Financial Force may use or disclose the personal information for the purposes of making the determination under paragraph 10.1.

10.3 If Financial Force:

(a) determines that it could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record,

Financial Force must as soon as practicable, destroy the information or ensure that the information is de-identified, only if it is lawful and reasonable to do so.

SECTION E – NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

11. NOTIFICATION OF COLLECTION

11.1 This section 11 applies to:

(a) solicited information; and

(b) unsolicited information to which section 10 does not apply.

11.2 Financial Force must notify the individual of the following matters in the Privacy Statement:

(a) Financial Force's identity and contact details;

(b) if Financial Force collects the personal information from a third party or the individual is not aware that Financial Force has collected the personal information, the fact that Financial Force so collects, or has collected the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a Court/Tribunal order, the fact that the collection is so required or authorised (including the details of the law or court);

(d) the purposes for which Financial Force collects the personal information;

(e) the main consequences (if any) for the individual if the information is not collected by Financial Force;

(f) any other entities to which Financial Force usually discloses personal information of the kind collected by Financial Force;

(g) that Financial Force's Privacy Statement and this Privacy Policy contains information about how the individual may access the personal information about the individual that is held by Financial Force and seek correction of such information;

(h) that Financial Force's Privacy Statement contains information about how the individual may complain about a breach of the Australian Privacy Principles and how Financial Force will deal with such a complaint;

(i) whether Financial Force will disclose the personal information to overseas recipients; and

(j) if Financial Force discloses the personal information to overseas recipients – the countries in which such recipients will be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

SECTION F – USE OR DISCLOSURE OF PERSONAL INFORMATION

12. USE OR DISCLOSURE

12.1 Where Financial Force holds personal information about an individual that was collected for a particular purpose ("**the primary purpose**"), Financial Force must not use or disclose the information for another purpose ("**the secondary purpose**") unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) the individual would reasonably expect Financial Force to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) directly related to the primary purpose (if the information is sensitive information); or

(ii) related to the primary purpose (if the information is *not* sensitive information);

(c) the use or disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

(d) a permitted general situation exists in relation to the use or disclosure of the information by Financial Force; or

(e) Financial Force reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

12.2 Where Financial Force uses or discloses personal information in accordance with section 12.1(e), Financial Force will keep a copy of this disclosure (e.g.: the email or letter used to do so).

12.3 This section 12 does not apply to:

(a) personal information for the purposes of direct marketing; or

(b) government related identifiers.

12.4 If Financial Force collects personal information from a related body corporate, this section 12 applies as if Financial Force's primary purpose for the collection was the primary purpose for which the related body corporate collected the information.

13. WHO DOES FINANCIAL FORCE DISLCOSE PERSONAL INFORMATION TO?

13.1 Financial Force may disclose personal information collected from clients and prospective clients to the following:

(a) organisations involved in providing, managing or administering Financial Force's product or service such as third-party suppliers, e.g. printers, posting services, and our advisers;

(b) organisations involved in maintaining, reviewing and developing Financial Force's business systems, procedures and infrastructure, including testing or upgrading Financial Force's computer systems;

(c) organisations involved in a corporate re-organisation;

(d) organisations involved in the payments system, including financial institutions, merchants and payment organisations;

(e) organisations involved in product planning and development;

(f) other organisations, who jointly with Financial Force, provide its products or services;

(g) authorised representatives who provide Financial Force's products or services on its behalf;

(h) the individual's representatives, including your legal advisers;

(i) debt collectors;

(j) Financial Force's financial advisers, legal advisers or auditors;

(k) fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;

(l) external dispute resolution schemes;

(m) regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

(n) Credit Reporting Bodies.

14. DISCLOSURE TO CREDIT REPORTING BODIES TO COMPLY WITH AML/CTF LEGISLATION

14.1 To enable Financial Force to comply with its obligations under the AML/CTF Legislation, Financial Force may disclose any or all of the following information to a Credit Reporting Body:

(a) the individual's name;

(b) the individual's residential address; and

(c) the individual's date of birth;

for the purposes of requesting a Credit Reporting Body provide an assessment of whether the information matches the information held by the Credit Reporting Body.

14.2 Prior to making a request to a Credit Reporting Body in accordance with section 14.1 above Financial Force:

(a) gives the individual information about:

(a) the reasons for Financial Force making the request to the Credit Reporting Body;

(b) the information about the individual that may be disclosed to the Credit Reporting Body;

(c) the fact that Financial Force may request the Credit Reporting Body to provide an assessment of whether the information matches (in whole or part) information held by the Credit Reporting Body;

(d) the fact that the Credit Reporting Body may prepare and provide to Financial Force such an assessment; and

(e) the fact that the Credit Reporting Body may use the information about the individual, and information held by the body that is the names, residential addresses and dates of birth of other individuals, for the purpose of preparing such an assessment; and

(b) ensures the individual has expressly agreed to the making of the request and the disclosure of the information; and

(c) makes available to the individual an alternative means of verifying the identity of the individual.

14.3 Upon receipt of an assessment of whether the information obtained by Financial Force matches the information held by the Credit Reporting Body and Financial Force is unable to verify the identity of the individual, having regard to the assessment, Financial Force must give written notice to the individual:

(a) stating that Financial Force is unable to verify the identity of the individual having regard to the assessment;

(b) specifying the name of the Credit Reporting Body that provided the assessment; and

(c) offering the individual an alternative means of verifying the identity of the individual.

14.4 Financial Force must keep the following records under this section 14:

(a) the name of the Credit Reporting Body to which the request was made;

(b) the information about the individual that was provided by Financial Force to the Credit Reporting Body;

(c) the assessment (if any) provided by the Credit Reporting Body in relation to the individual; and

(d) such other information about the verification request as is specified in the AML/CTF Legislation;

until the end of the first seven (7) year period:

(a) that began at a time after the verification request was made; and

(b) throughout the whole of which the Financial Force did not provide any services to the individual.

SECTION G – DIRECT MARKETING

15. DIRECT MARKETING

15.1 Financial Force must not use or disclose the personal information it holds about an individual for the purpose of direct marketing.

16. EXCEPTION – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION

16.1 Financial Force may use or disclose personal information (other than sensitive information) about an individual for the purposes of direct marketing if:

(a) Financial Force collected the information from the individual; and the individual would reasonably expect Financial Force to use or disclose the information for that purpose; or

(b) Financial Force has collected the information from a third party; and either:

(i) Financial Force has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or

(ii) it is impracticable for Financial Force to obtain the individual's consent; and

(c) Financial Force provides a simple way for the individual to opt out of receiving direct marketing communications from Financial Force;

(d) in each direct marketing communication with the individual Financial Force:

(i) includes a prominent statement that the individual may make such a request; or

(ii) directs the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made a request to opt out of receiving direct marketing.

17. EXCEPTION – SENSITIVE INFORMATION

17.1 Financial Force may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

18. REQUESTS TO STOP DIRECT MARKETING

18.1 Where Financial Force uses or discloses personal information about an individual for the purposes of direct marketing by Financial Force or facilitating direct marketing by another organisation, the individual may request:

(a) that Financial Force no longer provide them with direct marketing communications;

(b) that Financial Force does not use or disclose the individual's personal information for the purpose of facilitating direct marketing by another organisation;

(c) that Financial Force provides the source of the personal information.

18.2 Where Financial Force receives a request from an individual under section 18.1, Financial Force will:

(a) give effect to the request under section 18.1(a) or 18.1(b) within a reasonable period after the request is made and free of charge; and

(b) notify the individual of the source of the information, if the individual requests it, unless it is impracticable or unreasonable to do so.

18.3 This Section G does not apply to the extent that the following laws apply:

(a) the Do Not Call Register Act 2006;

(b) the Spam Act 2003; or

(c) any other Act of the Commonwealth of Australia.

SECTION H – CROSS BORDER DISCLOSURE OF PERSONAL INFORMATION

19. DISCLOSING PERSONAL INFORMATION TO CROSS BORDER RECIPIENTS

19.1 Where Financial Force or its Authorised Representatives discloses personal information about an individual to a recipient who is not in Australia and who is not Financial Force or the individual, Financial Force or its Authorised Representatives must ensure that the overseas recipient does not breach the Australian Privacy Principles (with the exception of APP1).

19.2 The countries we may disclose an individual's personal information to include:

(a) Reinsurers who may be based in Asia or America;

(b) Outsourced Administration Team who may be based in Asia.

19.3 Section 19.1 does not apply where:

(a) Financial Force reasonably believes that:

(i) information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) Financial Force has informed the individual that if they consent to the disclosure of information Financial Force will take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles; and

(ii) after being so informed, the individual consents to disclosure;

(c) the disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A (1) Privacy Act) exists in relation to the disclosure of the information by Financial Force.

SECTION I – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT IDENTIFIERS

20. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS

20.1 Financial Force must not adopt a government related identifier of an individual as its own identifier unless:

(a) Financial Force is required or authorised by or under an Australian law or a Court/Tribunal order to do so; or

(b) the identifier, Financial Force and the circumstances of the adoption are prescribed by regulations.

21. USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

21.1 Before using or disclosing a government related identifier of an individual, Financial Force must ensure that such use or disclosure is:

(a) reasonably necessary for Financial Force to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) required or authorised by or under an Australian law or a Court/Tribunal order; or

(d) within a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A (1) Privacy Act; or

(e) reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) the identifier, Financial Force and the circumstances of the adoption are prescribed by regulations.

SECTION J – INTEGRITY OF PERSONAL INFORMATION

22. QUALITY OF PERSONAL INFORMATION

22.1 Financial Force or its Authorised Representatives will ensure that the personal information it collects and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

23. SECURITY OF PERSONAL INFORMATION

23.1 Financial Force or its Authorised Representatives ensures that it protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure.

23.2 Financial Force or its Authorised Representatives takes reasonable steps to destroy or de-identify any personal information it holds where:

(a) Financial Force no longer needs the personal information for any purpose for which the information may be used or disclosed by Financial Force;

(b) the information is not contained in a Commonwealth record;

(c) Financial Force is not required to retain that information under an Australian law, or a Court/Tribunal order.

24. STORAGE OF PERSONAL INFORMATION

24.1 Financial Force or its Authorised Representatives stores personal information in different ways, including:

(a) hard copy on site at Financial Force or its Authorised Representatives' office;

(b) electronically secure data centres including Customer Relationship Management systems which are located in Australia and owned by either Financial Force or its Authorised Representatives or external service providers;

24.2 In order to ensure Financial Force protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure, Financial Force implements the following procedure/system:

(a) access to information systems is controlled through identity and access management;

(b) employees are bound by internal information securities policies and are required to keep information secure;

(c) all employees are required to complete training about information security;

(d) Financial Force regularly monitors and reviews its compliance with internal policies and industry best practice;

SECTION K – ACCESS TO, AND CORRECTION OF, PESRONAL INFORMATION

25. ACCESS

25.1 Financial Force must give an individual access to the personal information it holds about the individual if so requested by the individual.

25.2 Financial Force must respond to any request for access to personal information within a reasonable period after the request is made.

25.3 Financial Force must give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so and must take such steps as are reasonable in the circumstances to give access in a way that meets the needs of Financial Force and the individual.

25.4 Financial Force must not charge an individual for making a request and must not impose excessive charges for the individual to access their personal information.

26. EXCEPTIONS

26.1 Financial Force is not required to give an individual access to their personal information if:

(a) Financial Force reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access if frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between Financial Force and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal intentions of Financial Force in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a Court/Tribunal order; or

(h) Financial Force has reason that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within Financial Force in connection with a commercially sensitive decision-making process.

27. REFUSAL TO GIVE ACCESS

27.1 If Financial Force refuses to give access in accordance with section 25 or to give access in the manner requested by the individual, Financial Force will give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

27.2 Where Financial Force refuses to give access under section 26.1(j) Financial Force may include an explanation of the commercially sensitive decision in its written notice of the reasons for denial.

SECTION L – CORRECTION OF PERSONAL INFORMATION

28. CORRECTION OF INFORMATION

28.1 Financial Force must take reasonable steps to correct all personal information, having regard to the purpose for which the information is held where:

(a) Financial Force is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(b) the individual requests Financial Force corrects the information.

28.2 Where Financial Force corrects personal information about an individual that Financial Force previously disclosed to another APP entity and the individual requests Financial Force to notify the other APP entity of the correction, Financial Force must take reasonable steps to give that notification, unless it is impracticable or unlawful to do so.

29. REFUSAL TO CORRECT INFORMATION

29.1 If Financial Force refuses to correct personal information as requested by the individual, Financial Force will give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

30. REQUEST FROM A CLIENT TO ASSOCIATE A STATEMENT WITH THEIR INFORMATION

30.1 If:

(a) Financial Force refuses to correct personal information as requested by the individual; and

(b) the individual requests that Financial Force associate a statement noting that the information is inaccurate, out of date, incomplete, irrelevant or misleading, with the individual's information,

Financial Force must take such steps as are reasonable in the circumstances to associate the statement (as described in section 30.1(b)) with the individual's personal information. The statement should be associated with the information in such a way that will make the statement apparent to users of the information.

31. DEALING WITH REQUESTS

31.1 Financial Force must:

(a) respond to requests under this Section L within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

SECTION M – MAKING A PRIVACY COMPLAINT

32. COMPLAINTS

32.1 Financial Force offers a free internal complaint resolution scheme to all customers. Should a client have a privacy complaint, they are to contact Financial Force to discuss their concerns using the following contact details:

(a) Email: compliance@financialforce.com.au

(b) Phone: (07) 3210 0244

(c) Post: PO Box 12026 George Street BRISBANE QLD 4003

32.2 To assist Financial Force in helping customers, Financial Force asks customers to follow a simple three-step process:

(a) gather all supporting documents relating to the complaint;

(b) contact Financial Force to review your situation and if possible, resolve your complaint immediately; and

(c) if the matter is not resolved to the customer's satisfaction, customers are encouraged to contact Financial Force's Complaints Officer on (07) 3210 0244 or put their complaint in writing and send it to PO Box 12026 George Street BRISBANE QLD 4003.

32.3 Financial Force will rectify any breach if the complaint is justified and takes necessary steps to resolve the issue.

32.4 In certain situations, to deal with a complaint it may be necessary to consult with third parties. However, any disclosure of Personal Information to third parties will be provided with the customer's authority and consent.

32.5 After a complaint has been received, Financial Force sends the customer a written notice of acknowledgement setting out the process. The complaint is investigated, and the decision sent to the customer within thirty (30) days unless the customer has agreed to a longer time. If a complaint cannot be resolved within the agreed time frame or a decision could not be made within thirty (30) days of receipt, a notification will be sent to the customer setting out the reasons and specifying a new date when the customer can expect a decision or resolution.

32.6 If the customer is not satisfied with Financial Force's internal privacy practices or the outcome in respect to complaint, the customer may approach the OAIC with their complaint:

Office of the Australian Information Commissioner

Address: GPO Box 5218, Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Website: oaic.gov.au

SECTION N – MISCELLANEOUS

33. NOTIFIABLE DATA BREACHES SCHEME

33.1 Under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* ("**Privacy Amendment Act**") Financial Force is required to notify the Office of the Australian Information Commissioner ("**OAIC**") in relation to all eligible data breaches.

33.2 Financial Force must notify the OAIC by lodging a Notifiable Data Breach Form soon as practicable. The Notifiable Data Breach Form is available at the following link: https://webform.oaic.gov.au/prod?entitytype=DBN&layoutcode=DataBreachWF

33.3 Under the Privacy Amendment Act, Financial Force must also promptly inform clients whose personal information has been compromised by the eligible data breach that a breach of their personal information has occurred.

34. POLICY BREACHES

34.1 Breaches of this Policy may lead to disciplinary action being taken against the relevant party, including dismissal in serious cases and may also result in prosecution under the law where that act is illegal. This may include re-assessment of bonus qualification, termination of employment and/or fines (in accordance with the Privacy Act).

34.2 Staff are trained internally on compliance and their regulatory obligation to Financial Force. They are encouraged to respond appropriately to and report all breaches of the law and other incidents of non-compliance, including Financial Force's policies, and seek guidance if they are unsure.

34.3 Staff must report breaches of this Policy directly to the Director.

35. RETENTION OF FORMS

35.1 The Compliance Officer will retain the completed forms for seven (7) years in accordance with Financial Force's Document Retention Policy. The completed forms are retained for future reference and review.

35.2 As part of their training, all staff are made aware of the need to practice thorough and up to date record keeping, not only as a way of meeting Financial Force's compliance obligations, but as a way of minimising risk.

36. POLICY REVIEW

36.1 Financial Force's Privacy Policy will be reviewed on at least an annual basis by the Compliance Officer of Financial Force, having regard to the changing circumstances of Financial Force. The Compliance Officer will then report to the Director on compliance with this Policy.

Issued by Financial Force 28/10/2021

Reviewed on 31/10/2026