POL 3005.25
Privacy Policy

Version:	6.2
Effective Date:	1 April 2026
Administered by:	Executive Manager Risk & Compliance
Reviewed by:	Compliance and Operational Risk Committee and Board Risk Committee
Approved by:	Board

References

Australian Privacy Principles
Customer Owned Banking Code of Practice
Do Not Call Register Act 2006
Privacy Act 1988
Spam Act 2003
Police Credit Union Privacy Policy Statement
Ian Berry Insurance Services Privacy Policy Statement
INF 3005.25 Privacy - Document Access and Correction
POL 1425 Counselling and Disciplinary Policy
POL 2610 Staff and Related Accounts Policy
POL 3002.14 Technology and Information Security Policy
POL 2350 Service Provider Management Policy Framework
POL 3002.18 Information Classification Policy
POL 3005.39 Code of Ethics Policy
PRO 3005.25 Notifiable Data Breaches
IT Security Incident - Response Plan and Checklist
FRM 2350.1 Contract Checklist
Data Breach Assessment Report
Crisis Management Communication Plan
Incident Management Plan
Business Continuity Plan

Definitions and Interpretations

Eligible Data Breach – an Eligible Data Breach arises when the following three criteria are satisfied:

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that Police Credit Union (**PCU**) holds;
2. This is likely to result in serious harm to one or more individuals; and
3. PCU has not been able to prevent the likely risk of serious harm with remedial action.

PCU must notify the OAIC of Eligible Data Breaches in accordance with this Policy.

OAIC – Office of the Australian Information Commissioner (The Privacy Regulator)

PCU Employees – all employees of Police Credit Union, including directors and contractors

PCU – Police Credit Union

Overview

This policy establishes the requirements for the collection, use, disclosure, storage and protection of personal information at PCU.

PCU complies with the Privacy Act 1988 including the Australian Privacy Principles contained within, and other relevant obligations such as those in the Spam Act 2003, the Do Not Call Register Act 2006, and the Customer Owned Banking Code of Practice.

Detailed below are the standards that **PCU Employees** must maintain to ensure personal information is handled lawfully, securely, and in a manner that maintains member trust.

Policy

Access and Disclosure of Personal Information

PCU Employees are expressly forbidden from accessing or attempting to access Member accounts (including those of other PCU Employees) without a clear business purpose or the express consent of the member. All **PCU Employee's** must not access, use or disclosure personal information except where:

- It is required to perform their role; and
- It is in accordance with this policy and the *Privacy Act 1988*.

All PCU Employees must submit requests for access to other PCU Employee accounts via OTRS to the **Risk & Compliance Department** who will review the request and remove the protection, where warranted, to allow temporary access to the account to conduct the task required in their job role. The **Risk & Compliance Department** will monitor access to accounts and investigate and report any misuse or inappropriate access on accounts.

Third Party Suppliers

Prior to entering into a contract with a third party, the relevant **Executive Manager** and the **Executive Manager Technology & Data** must undertake an assessment of the third party and the classification of information they will have access to, in accordance with POL3002.18 Information Classification Policy.

Executive Managers must ensure that, in accordance with POL 2350 Service Provider Management Policy Framework and as documented in FRM 2350.1 Contract Checklist, where a contract with a third party will involve that party accessing or receiving PCU information, which may include personal information of members, the contract must specify various requirements for the protection of that information, including confidentiality and non-disclosure requirements, and the third party's security controls and required processes in the event of a data breach.

Disclosure Documents

In meeting the requirements under the Australian Privacy Principles, **PCU Employees** must provide, or make available where applicable, the required privacy disclosure documents to members, applicants or other individuals or entities. The 3 prescribed privacy disclosure documents are:

- **PCU/IBIS Privacy Policy Statements:** must be posted on PCU's and Ian Berry websites and be made available on request.
- **Privacy Notice:** must be provided to all new members and prospective members.
- **Loan Privacy Permission Form:** must be provided to all members and prospective members on application for credit.

Data Breaches

PCU has in place strong data security practices as set out in POL 3002.14 Technology and Information Security Policy. If unauthorised access to, unauthorised disclosure of, or loss of personal information occurs despite these strong data security practices, **PCU Employees** must immediately take action to recover the information, minimise harm to the impacted member(s) and PCU, and prevent further loss of information.

Actions which must be taken are set out in POL 3002.14 Technology and Information Security Policy, the IT Security Incident – Response Plan and Checklist, PRO 3005.25 Notifiable Data Breaches and, where required, the Crisis Management Communication Plan.

All suspected or actual data breaches must be reported to the **Risk & Compliance Department** using the 'Report an Operational Incident' form on MyPCU as soon as possible and in any event not longer than 24 hours of the PCU Employee becoming aware of the data breach. Examples of what may constitute a data breach are set out in PRO 3005.25 Notifiable Data Breaches.

The **Risk & Compliance Department** must then:

- investigate the data breach to determine what steps have already been taken to address the data breach and what further steps should be undertaken to reduce the likelihood of serious harm to an impacted individual or individuals;
- complete a Data Breach Assessment Report;
- if further steps are required, liaise with the relevant **Executive Manager** to ensure recommended steps are undertaken in a timely manner; and
- undertake an assessment in accordance with PRO 3005.25 Notifiable Data Breaches as to whether the breach is an Eligible Data Breach requiring notification to the OAIC.

If it is the opinion of the Risk & Compliance Department that the breach constitutes an Eligible Data Breach and therefore requires notification to the OAIC, the **Executive Manager Risk & Compliance** will first obtain agreement from the **CEO** and relevant **Executive Manager**. If in agreement, notification to the OAIC will be submitted within 30 days of first awareness of the breach. Any impacted individual(s), or where relevant, the general public, must also be notified of an Eligible Data Breach, which will be managed in conjunction with the **CEO** and/or **Executive Manager Brand, Marketing & Communications**.

Breaches of this Policy

The relevant **Executive Manager** and the **Executive Manager People & Culture** will ensure that Employees who do not comply with the obligations of this policy is subject to disciplinary action in accordance with POL 1425 Counselling and Disciplinary Policy, and which may include the termination of their employment as per POL 3005.15 Summary Dismissal Policy and/or potential legal prosecution.

Annual Policy and Control Attestation:

In completing this attestation and as the Responsible Officer for the implementation of this policy, I confirm that following reasonable enquiries and to the best of my knowledge, other than previously reported exceptions and/or those provided in support of this attestation, each listed policy requirement has been completed. Any known material exceptions have been reported to the Chief Executive Officer and the Chief Risk Officer.

Angela Scarfo

Signed

Angela Scarfo Executive Manager Risk & Compliance, dated 27 February 2026

Version Control – Material Changes

Version Number	Effective Date	Changes
1.0 – 6.1	26 March 2025	Prior versions
6.2	1 April 2026	Non-Material changes