Southern Mutual Bank

51 824 753 556

Personal Information Handling Procedure

Procedure · synthetic assessor-grade test document

Generated 09 November 2026 · CyberSentien test harness · personalised to Southern Mutual Bank

Document ID	SOU-PRO-0047
Version	3.2
Owner	Daniel Wright (Business Continuity Manager)
Approved by	CISO
Classification	Internal Use Only
Status	Approved — In force
Effective date	14 Mar 2026
Next review	14 Mar 2027

1. Purpose and control objectives

This procedure establishes the requirements, accountabilities and control objectives for personal information handling procedure across Southern Mutual Bank (“the Bank”). It forms part of the Bank's Information Security Management System and supports its obligations under NDB Scheme, APRA CPS 234, ISO/IEC 27001:2022. It applies to Core banking platform and supporting services.

Control objectives:

• Protect personal information and other sensitive records throughout their lifecycle through documented handling, records management and record retention rules.

• Maintain documentation of what information is held, where, why and for how long, so retention periods and disposal are demonstrable.

• Support privacy rights, legal hold and regulatory record-keeping obligations with documented procedures and evidence.

2. Scope

This document applies to all employees, contractors, temporary staff and third parties acting for Southern Mutual Bank, and to all information assets, systems and environments it operates or operates on its behalf — on-premise, cloud (AWS/Azure), SaaS and outsourced services.

In scope	Out of scope / exclusions
Production, management and DR environments; Core banking platform; identity, endpoint, network and data services.	Personal devices outside the BYOD programme; non-production sandboxes without Bank data (covered by separate standard).

3. Regulatory and standards context

The requirements herein are designed to satisfy, and are crosswalked to, the following frameworks applicable to a regulated Australian banking entity: NDB Scheme, APRA CPS 234, ISO/IEC 27001:2022. Where an obligation is

more stringent in one framework, the most stringent requirement applies.

4. Requirements

4.1 Information handling and data protection

4.1.1 Personal information and other sensitive records shall be handled per their classification: collected only for a documented purpose, accessed on a need-to-know basis, encrypted in transit and at rest, and never sent to unapproved services or personal accounts.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. log + exception review. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.2 Data protection controls (masking, pseudonymisation, data loss prevention) shall be applied where personal information is used outside the production system of record.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. configuration review + sampling. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.3 Transfers of personal information to third parties or across borders shall be authorised, covered by contract and recorded in the transfer register.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.1.4 Records of processing shall document each processing activity: purpose, data categories, data subjects, recipients, retention period and safeguards.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. log + exception review. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2 Records management and documentation

4.2.1 A records management framework shall define what constitutes a record, the system of record for each record class, ownership and the documented procedures for creating, capturing, classifying and storing records.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.2 Documentation of systems, processes and controls shall be maintained under document control: unique identifier, version, owner, approval and review date.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.3 Records shall be captured in approved systems (not personal drives or email) with metadata sufficient to find, retrieve and prove authenticity.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.4 Standard operating procedures for record keeping shall be published, trained and reviewed at least annually.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. log + exception review. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.3 Record retention and disposal

4.3.1 A records retention schedule shall define the retention period for every record class, derived from legal, regulatory (including APRA and the Privacy Act) and business requirements, and approved by Legal.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.2 Records shall be retained for their retention period and no longer; over-retention of personal information is prohibited and shall be reported as a privacy compliance gap.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.3.3 Disposal shall follow the retention schedule and be authorised, logged and irreversible: secure deletion for electronic records and secure destruction for paper and media, with a certificate of destruction retained.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.4 Legal hold shall suspend disposal for records relevant to litigation, investigation or regulatory enquiry until released in writing by Legal.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4 De-identification, aggregation and audit-record minimisation

4.4.1 Personal information used for analytics, reporting, testing or AI training shall be de-identified before use: direct identifiers removed, quasi-identifiers generalised or suppressed, and re-identification risk assessed and recorded.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.4.2 Statistics and aggregate results published or reported outside the system of record shall have differential privacy applied — calibrated non-deterministic noise added to the results of the mathematical operations before the results are reported — so that no individual's personal information can be inferred from a published figure.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.3 Personally identifiable information contained in audit records and event logs shall be limited to the elements identified in the privacy risk assessment for that system (user identifier, timestamp, action, object); names, contact details and identity document numbers shall not be written to audit records.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. log + exception review. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.4 Third-party disclosures of personal information shall occur only under an agreement with appropriate protections, and a record of authorised disclosures (recipient, date, purpose, authority) shall be created and retained in the disclosure register.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5 Privacy rights, access and correction

4.5.1 Requests by individuals to access or correct their personal information shall be verified, logged and fulfilled within statutory timeframes through the documented procedure.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.2 Complaints and enquiries about the handling of personal information shall be recorded, investigated and answered, with trends reported to the Privacy Officer quarterly.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. automated telemetry review. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.3 Privacy impact assessments shall be completed and recorded for new or materially changed processing of personal information.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.4 Personal information used for testing, analytics or AI training shall be de-identified or explicitly authorised and documented.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.6 Assurance of record keeping

4.6.1 Record-keeping compliance shall be sampled quarterly: capture in the system of record, correct classification, retention applied and disposal evidenced.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6.2 Privacy and records management incidents shall be managed under the incident response plan and, where eligible, assessed for notification under the Notifiable Data Breaches scheme.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. log + exception review. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6.3 The records inventory, retention schedule and records of processing shall be reviewed annually and after material change.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.7 Records in cloud and collaboration services

4.7.1 Records held in SaaS and collaboration platforms shall be subject to the same retention schedule, applied through the platform's retention labels and verified quarterly.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7.2 Personal information shall not be retained in chat, email or personal storage beyond the retention period; automated retention policies shall enforce this.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.7.3 Exports of records from cloud services for migration or decommissioning shall be authorised, logged and disposed of when the migration is complete.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. log + exception review. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.8 Governance, accountability and policy lifecycle

4.8.1 A named executive owner shall be accountable for this control area and shall report its status to the Board Risk Committee at least quarterly.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.8.2 This document shall be reviewed at least annually and after any material change to the business, technology, regulatory or threat environment, with version control maintained.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. re-performance / observation. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.8.3 Roles and responsibilities shall align to the three-lines-of-defence model, with first-line ownership, second-line oversight and third-line independent assurance.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.8.4 Material decisions, approvals and deviations shall be minuted and retained as part of the governance record.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. automated telemetry review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.9 Risk assessment and treatment

4.9.1 Risks within this control area shall be identified, assessed (likelihood × impact), treated and recorded in the enterprise risk register with an accountable owner.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. automated telemetry review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.9.2 Residual risk exceeding the approved risk appetite shall be escalated with a treatment plan and target date.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.9.3 Risk assessments shall be refreshed on a defined cadence and upon significant change.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.9.4 Key risk indicators (KRIs) shall be defined and monitored against thresholds, with breaches escalated.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10 Monitoring, measurement and reporting

4.10.1 Control performance shall be monitored continuously through automated telemetry into the central assurance platform.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. automated telemetry review. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10.2 The metrics and targets in this document shall be reported monthly to the control owner and quarterly to the Executive Risk Committee.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the

hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. configuration review + sampling. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10.3 Control failures and exceptions shall be logged, triaged by severity and remediated within risk-based timeframes.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10.4 Independent assurance (internal audit / external assessment) shall periodically test design and operating effectiveness; findings shall be tracked to closure.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. automated telemetry review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.11 Records, retention and evidence

4.11.1 Evidence demonstrating the operation of these controls shall be generated, retained and protected per the records-retention schedule.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.11.2 Evidence shall be sufficient for an independent assessor to conclude on operating effectiveness without reliance on undocumented knowledge.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. re-performance / observation. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.11.3 Access to control evidence shall be least-privilege and itself logged; integrity shall be protected against tampering.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.11.4 On decommissioning, records shall be retained or disposed of per the retention schedule and legal hold requirements.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. configuration review + sampling. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.12 Continuous improvement

4.12.1 Lessons from incidents, audits, assessments and exercises shall be fed back into this control area and the document updated accordingly.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. automated telemetry review. *Frequency.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.12.2 Control maturity shall be assessed against a defined target state, with a roadmap to close gaps.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.12.3 Automation and tooling shall be progressively adopted to reduce manual effort and error.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. log + exception review. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Business Continuity Manager	✓	✓			Owns this document; ensures it is current, resourced and effective.
System / Asset owners	✓		✓		Implement and operate the controls in their scope.
Security Operations	✓		✓	✓	Monitors compliance; investigates and responds to exceptions.
Risk & Compliance (2nd line)			✓	✓	Provides oversight, challenge and reporting.
Internal Audit (3rd line)				✓	Independent assurance over design and operating effectiveness.

Role	R	A	C	I	Responsibility
All staff & contractors	✓			✓	Comply with the requirements; report suspected breaches.

6. Procedures and implementation

6.1 Information owner registers a new record class or processing activity in the records inventory with purpose, classification, system of record and retention period.

6.2 Records Management applies the retention schedule in the system of record; disposal runs are approved by the information owner and logged with a certificate of destruction.

6.3 Privacy Office verifies an access or correction request, retrieves the records, redacts third-party information and responds within the statutory period.

6.4 Legal issues and releases legal holds in writing; Records Management suspends and resumes disposal accordingly.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Record classes with an approved retention period	100%	Annual
Records disposed within 90 days of retention expiry	≥ 95%	Quarterly
Access and correction requests answered within statutory period	100%	Monthly
Processing activities with a current record of processing	100%	Quarterly
Privacy impact assessments completed for in-scope changes	100%	Quarterly

8. Compliance, monitoring and enforcement

Compliance is monitored continuously through automated control telemetry, the metrics above and periodic independent assurance. Material non-compliance is recorded in the risk register, escalated to the Executive Risk Committee, and tracked to closure. Wilful or negligent breaches may result in disciplinary action up to termination.

9. Exceptions and waivers

Any deviation requires a documented risk assessment, compensating controls, an expiry date and approval by the accountable risk owner (and the CISO for high-risk deviations). Active exceptions are recorded and reviewed in the Exceptions & Waivers Register.

10. Definitions

Term	Definition
Record	Information created or received as evidence of a business activity and retained under the retention schedule.
Retention period	The minimum and maximum time a record class is kept before authorised disposal.
Record of processing	Documentation of a personal-information processing activity: purpose, data, recipients, retention, safeguards.
Legal hold	A written instruction suspending disposal of records relevant to a legal or regulatory matter.

11. Related documents

- Privacy Policy
- Data Retention & Disposal Standard
- Data Classification & Handling Standard

• Records Management & Data Handling Procedure

12. Control framework mapping

Framework	Indicative mapped controls
NDB Scheme	Assessment, Notification
APRA CPS 234	Information security capability, Control testing, Incident notification
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23

Threat and risk context

This control area addresses the threats and failure modes most relevant to Core banking platform in a regulated Australian banking context — including credential compromise, insider misuse, unmanaged change, third-party failure, data loss and control drift. The requirements in section 4 are calibrated to reduce both the likelihood and the impact of these scenarios, and are tested on the cadence set out in section 7.

• Risk addressed: Protect personal information and other sensitive records throughout their lifecycle through documented handling, records management and record retention rules.

• Risk addressed: Maintain documentation of what information is held, where, why and for how long, so retention periods and disposal are demonstrable.

• Risk addressed: Support privacy rights, legal hold and regulatory record-keeping obligations with documented procedures and evidence.

Operating model and continuous assurance

Day-to-day operation follows the three-lines-of-defence model: first-line owners operate the controls and remediate exceptions; second-line risk and compliance provide oversight, challenge and reporting; third-line internal audit provides independent assurance. Control performance is monitored continuously through automated telemetry into the central assurance platform, with monthly control reporting to the control owner and quarterly reporting to the Executive Risk Committee. Deficiencies are recorded in the enterprise risk register and tracked to closure against the targets in section 7.

Training, awareness and competency

Personnel with responsibilities under this document receive role-based training at onboarding and at least annually. General security awareness, including phishing simulation, is delivered to all staff and contractors; completion is tracked and non-completion is escalated to people leaders. Control owners maintain procedures and runbooks sufficient for a competent operator to execute the control consistently, and review them after any material change to the business, technology or threat environment.

Appendix C — Control register (per requirement)

Ref	Control statement	Framework	Test freq.	Status
4.1.1	Personal information and other sensitive records shall be handled per …	NDB Scheme	Quarterly	Implemented
4.1.2	Data protection controls (masking, pseudonymisation, data loss prevent…	APRA CPS 234	Quarterly	Implemented
4.1.3	Transfers of personal information to third parties or across borders s…	ISO/IEC 27001:2022	Semi-annual	Partially implemented
4.1.4	Records of processing shall document each processing activity: purpose…	NDB Scheme	Quarterly	Implemented
4.2.1	A records management framework shall define what constitutes a record,…	APRA CPS 234	Semi-annual	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.2.2	Documentation of systems, processes and controls shall be maintained u…	ISO/IEC 27001:2022	Monthly	Implemented
4.2.3	Records shall be captured in approved systems (not personal drives or …	NDB Scheme	Monthly	Partially implemented
4.2.4	Standard operating procedures for record keeping shall be published, t…	APRA CPS 234	Monthly	Implemented
4.3.1	A records retention schedule shall define the retention period for eve…	ISO/IEC 27001:2022	Annual	Implemented
4.3.2	Records shall be retained for their retention period and no longer; ov…	NDB Scheme	Semi-annual	Implemented
4.3.3	Disposal shall follow the retention schedule and be authorised, logged…	APRA CPS 234	Annual	Implemented
4.3.4	Legal hold shall suspend disposal for records relevant to litigation, …	ISO/IEC 27001:2022	Semi-annual	Implemented
4.4.1	Personal information used for analytics, reporting, testing or AI trai…	NDB Scheme	Monthly	Implemented
4.4.2	Statistics and aggregate results published or reported outside the sys…	APRA CPS 234	Annual	Implemented
4.4.3	Personally identifiable information contained in audit records and eve…	ISO/IEC 27001:2022	Annual	Implemented
4.4.4	Third-party disclosures of personal information shall occur only under…	NDB Scheme	Quarterly	Implemented
4.5.1	Requests by individuals to access or correct their personal informatio…	APRA CPS 234	Quarterly	Partially implemented
4.5.2	Complaints and enquiries about the handling of personal information sh…	ISO/IEC 27001:2022	Monthly	Implemented
4.5.3	Privacy impact assessments shall be completed and recorded for new or …	NDB Scheme	Semi-annual	Implemented
4.5.4	Personal information used for testing, analytics or AI training shall …	APRA CPS 234	Quarterly	Implemented
4.6.1	Record-keeping compliance shall be sampled quarterly: capture in the s…	ISO/IEC 27001:2022	Quarterly	Partially implemented
4.6.2	Privacy and records management incidents shall be managed under the in…	NDB Scheme	Annual	Implemented
4.6.3	The records inventory, retention schedule and records of processing sh…	APRA CPS 234	Annual	Partially implemented
4.7.1	Records held in SaaS and collaboration platforms shall be subject to t…	ISO/IEC 27001:2022	Quarterly	Implemented
4.7.2	Personal information shall not be retained in chat, email or personal …	NDB Scheme	Annual	Implemented
4.7.3	Exports of records from cloud services for migration or decommissionin…	APRA CPS 234	Annual	Implemented
4.8.1	A named executive owner shall be accountable for this control area and…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.8.2	This document shall be reviewed at least annually and after any materi…	NDB Scheme	Quarterly	Implemented
4.8.3	Roles and responsibilities shall align to the three-lines-of-defence m…	APRA CPS 234	Monthly	Partially implemented

Ref	Control statement	Framework	Test freq.	Status
4.8.4	Material decisions, approvals and deviations shall be minuted and reta…	ISO/IEC 27001:2022	Monthly	Partially implemented
4.9.1	Risks within this control area shall be identified, assessed (likeliho…	NDB Scheme	Monthly	Implemented
4.9.2	Residual risk exceeding the approved risk appetite shall be escalated …	APRA CPS 234	Monthly	Partially implemented
4.9.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.9.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	NDB Scheme	Quarterly	Implemented
4.10.1	Control performance shall be monitored continuously through automated …	APRA CPS 234	Monthly	Implemented
4.10.2	The metrics and targets in this document shall be reported monthly to …	ISO/IEC 27001:2022	Quarterly	Implemented
4.10.3	Control failures and exceptions shall be logged, triaged by severity a…	NDB Scheme	Semi-annual	Implemented
4.10.4	Independent assurance (internal audit / external assessment) shall per…	APRA CPS 234	Annual	Implemented
4.11.1	Evidence demonstrating the operation of these controls shall be genera…	ISO/IEC 27001:2022	Monthly	Implemented
4.11.2	Evidence shall be sufficient for an independent assessor to conclude o…	NDB Scheme	Semi-annual	Partially implemented
4.11.3	Access to control evidence shall be least-privilege and itself logged;…	APRA CPS 234	Monthly	Partially implemented
4.11.4	On decommissioning, records shall be retained or disposed of per the r…	ISO/IEC 27001:2022	Monthly	Implemented
4.12.1	Lessons from incidents, audits, assessments and exercises shall be fed…	NDB Scheme	Annual	Implemented
4.12.2	Control maturity shall be assessed against a defined target state, wit…	APRA CPS 234	Monthly	Implemented
4.12.3	Automation and tooling shall be progressively adopted to reduce manual…	ISO/IEC 27001:2022	Monthly	Implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Information handling and data protection	4 control(s)	Implemented
Records management and documentation	4 control(s)	Planned
Record retention and disposal	4 control(s)	Planned
De-identification, aggregation and audit-record minimisation	4 control(s)	Planned
Privacy rights, access and correction	4 control(s)	Implemented
Assurance of record keeping	3 control(s)	Partially implemented
Records in cloud and collaboration services	3 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Implemented
Risk assessment and treatment	4 control(s)	Planned
Monitoring, measurement and reporting	4 control(s)	Implemented

Control area	Controls	Implementation status
Records, retention and evidence	4 control(s)	Implemented
Continuous improvement	3 control(s)	Planned

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Information handling and data protection	4	Configuration review + sampling	Config export + screenshots	Monthly
Records management and documentation	4	Automated control telemetry	Dashboard / telemetry extract	Annual
Record retention and disposal	4	Evidence inspection + interview	Approved records + tickets	Monthly
De-identification, aggregation and audit-record minimisation	4	Re-performance / observation	Observed run + sign-off	Quarterly
Privacy rights, access and correction	4	Log and exception review	SIEM / log extract	Monthly
Assurance of record keeping	3	Independent test / scan	Scan / test report	Annual
Records in cloud and collaboration services	3	Configuration review + sampling	Config export + screenshots	Semi-annual
Governance, accountability and policy lifecycle	4	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Risk assessment and treatment	4	Evidence inspection + interview	Approved records + tickets	Annual
Monitoring, measurement and reporting	4	Re-performance / observation	Observed run + sign-off	Semi-annual
Records, retention and evidence	4	Log and exception review	SIEM / log extract	Quarterly
Continuous improvement	3	Independent test / scan	Scan / test report	Annual

Evidence is retained for audit per the records-retention schedule and crosswalked to NDB Scheme, APRA CPS 234, ISO/IEC 27001:2022.

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	Daniel Wright	Business Continuity Manager	10 Oct 2026
Reviewed by	Mei-Lin Tan	IT Operations Manager	20 Oct 2026
Approved by	Priya Sharma	Chief Information Security Officer	26 Oct 2026
Endorsed by	—	Board Risk Committee	30 Oct 2026

Distribution: all staff and contractors via the policy portal; control owners; Risk & Compliance (2nd line); Internal Audit (3rd line); relevant material service providers under NDA.

14. Abbreviations

Abbreviation	Meaning
ISMS	Information Security Management System
MFA / SSO	Multi-Factor Authentication / Single Sign-On
PAM / IGA	Privileged Access Management / Identity Governance & Administration
RTO / RPO	Recovery Time Objective / Recovery Point Objective
SoD	Segregation of Duties
KRI / KPI	Key Risk Indicator / Key Performance Indicator

Abbreviation	Meaning
SIEM / SOC	Security Information & Event Management / Security Operations Centre

15. Revision history

Version	Date	Author	Summary of change
1.0	03 Oct 2023	Nadia Petrova	Initial issue.
2.0	02 Oct 2024	Greg Thompson	Annual review; control uplift and framework alignment.
3.2	02 Oct 2025	Daniel Wright	Updated for current framework versions and cloud scope.