Standard

medibank

Third Party Information Security Standard (External)

CONTENTS PAGE

1. INTRODUCTION

As a third party to Medibank Group, you play a vital role in protecting the security of our information, systems, and customers. This standard sets out the minimum-security requirements that all Medibank third parties must meet to reduce cybersecurity risks and ensure compliance with relevant laws and regulations.

Medibank's approach to information security is guided by our Information Security Policy Framework (ISPF), which is aligned with the Medibank Cyber Security Strategy. The ISPF outlines our security principles, roles, responsibilities, and the overarching approach to managing information security risk.

The ISPF includes the policies, standards, and procedures required to establish and maintain effective security controls. It is based on industry-recognised frameworks, obligations and regulatory requirements, including:

- The NIST Cybersecurity Framework (CSF)
- Payment Card Industry Data Security Standard (PCI-DSS)
- APRA Prudential Standard CPS 234 – Information Security
- APRA Prudential Standard CPS 230 – Operational Risk Management
- Privacy Act 1988
- Security of Critical Infrastructure Act 2018

Responsible, reliable, and respectful business practices are essential to building strong, mutually beneficial relationships with our third parties. As such, our third parties are expected to:

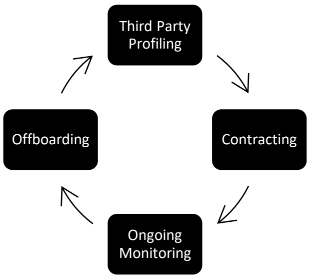
- comply with all applicable laws, regulations, and standards
- effectively manage risks within their operations and supply chain
- implement and maintain information security measures to protect Medibank's data
- report any breaches promptly in accordance with regulatory requirements and cooperate with regulatory investigations, audits, or requests related to their handling of Medibank data throughout their engagement lifecycle with Medibank.

2. SCOPE

This standard applies to all Medibank third parties, including suppliers, subcontractors, and service providers who process, store, transmit, or have access to Medibank data, systems, facilities, or technology. Compliance with this standard is required throughout the entire third-party engagement lifecycle, which includes:

- Profiling – Initial risk assessment and due diligence
- Contracting – Embedding security obligations into agreements
- Ongoing Monitoring – Regular review and assurance activities
- Offboarding – Secure termination of access and data handling

All third parties are expected to understand and adhere to the requirements outlined in this standard at every stage of their engagement with Medibank. Based on our third-party profiling, vendor security assessments are performed upon onboarding and periodically throughout the lifecycle of your engagement with us to ensure compliance with the requirements of this standard, and to ensure you have robust information security controls and capabilities in place to safeguard our data and assets.



3. ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Responsible	
Third Parties	• Maintain compliance with standard requirements. • Provide responses to the questionnaire requested by Medibank (Security Due Diligence/Security Assessment) and support questionnaire responses with supporting documentation as requested. • Permit Medibank assessors or their representatives to perform detailed control assessments to verify the third-party security control environment or provide independent assurance of control operation. • Develop and implement a remediation plan to address any controls gaps identified during the Security Due Diligence and/or Security Assessment. • Communicate the progress of the remediation plan. • Facilitate monitoring of services provided against service levels. • Report all security incidents related to Medibank in a timely manner.
Accountable	
Procurement	• Ensure that this standard is shared with third parties prior to onboarding the third parties and after any periodic updates to this standard.
Supportive	
Security Consulting	• Ensure that this standard is periodically reviewed and updated to reflect changes in requirements. • Offer expertise and advisory support from security perspective to Medibank stakeholder and third parties.
Consulted	
Legal	• Offer expertise and consulting from legal perspective to Medibank stakeholders and third parties.
Privacy	• Offer expertise and consulting from privacy perspective to Medibank stakeholders and third parties.
Informed	
All users	• Read, understand, and ensure ongoing adherence to this standard.

4. STANDARD REQUIRMENTS

The third parties providing services to Medibank must comply with below security requirements when accessing or managing Medibank data, systems, assets, property and locations.

ID	Domain	Requirement
1.	**APRA CPS 234 compliance**	• **Information Security Capability** - Third party must provide Medibank with access to relevant personnel, systems, and facilities upon reasonable request to assess its information security capabilities. • **Classification of Information Assets** - Medibank will classify assets managed by the Third party. Third party must treat assets according to their classification and mitigate risks based on the potential impact of a security incident. • **Third party to Implement Information Security Controls** - Third party must implement timely and appropriate security controls to protect Medibank's assets, based on asset sensitivity, risks, and potential impact of security incidents. Third party must provide Medibank access to systems and personnel to assess the effectiveness of these controls. Upon request, Third party must review and report on control effectiveness. Further, third party must promptly update controls to ensure adequate protection of Medibank's assets, as deemed necessary by Medibank. • **Third party to Implement Information Security Testing -** Third party must conduct regular security testing to evaluate control effectiveness, based on asset sensitivity, risk factors, and evolving threats. Third party must provide access to testing processes and systems upon request. • **Notification of Incidents and Weaknesses** - Third party must notify Medibank within 48 hours of a significant security incident or potential impact. Detailed information about the incident must be provided. Third party must report any security control weaknesses within two business days if not promptly remediated. Third party must seek Medibank's approval before notifying and other related parties and comply with Medibank's directions for notification, unless required by law.
2.	**Unauthorised Activities**	The Third Party must ensure their personnel do not engage in any of the following: • Accessing, using, sharing, storing, or transmitting confidential, personal, or sensitive data (e.g., financial, health, or payment card information) without proper authorisation. • Storing sensitive data unencrypted on local drives or removable devices. • Sending unencrypted sensitive or internal information through unsecured channels like email, instant messaging, or fax. • Sending phishing emails, hoaxes, spam, or junk messages. • Handling or distributing malicious software or code that could harm Medibank systems. • Sharing passwords or allowing others to use their accounts. • Trying to access systems using someone else's login details.

		• Saving passwords in web browsers or syncing browser data between work and personal devices. • Posting Medibank's personal or business information on public forums or community websites. • Tampering with or bypassing Medibank's security tools or controls without permission.
3.	**Physical and Data Centre Security**	The Third Party must ensure that they enforce below physical security and data centre security requirements: • **Physical Security** – Control access to buildings using secure methods (e.g. smart cards, key systems, biometrics). – Use video surveillance, alarm systems, and intrusion detection in sensitive areas. – Maintain CCTV coverage of sensitive areas with signage and compliance with privacy laws. – Visitors must register at Medibank reception and be accompanied by authorised personnel. – All personnel must wear visible ID badges on site. • **Data Centre Security** – Restrict access to data centre areas to authorised staff only. – Secure facilities with surveillance, guards, motion detectors. – Log and monitor all entries to data centre areas. – Store servers in secure, access-controlled rooms with no external wall exposure. – Maintain CCTV footage and ensure backup power is available for critical systems. – Make surveillance footage available upon request for incident investigation or disciplinary matters.
4.	**Access Control**	The Third Party must ensure that: • Access to Medibank information & system must be granted on a need-to know basis and follow the principle of least privilege. • User access must be reviewed periodically to ensure that access is required as granted and not being misused. • The access rights and/or user accounts (including both standard and privileged accounts) of third-party users supporting Medibank work must be suspended (disabled) on the same day their legitimate need for access ends (e.g., termination of employment, contract completion, or role change). • Suspended accounts must be permanently terminated (deleted) within 30 days of access suspension, ensuring no residual access to Medibank's network or resources. • Privileged access must be granted on an event-by-event basis or a need-to-use basis. • Role-based Access Control (RBAC) access provisioning must align with an authoritative source (e.g., Human Resources System) and be readily updated as position title changes. • Multi-factor authentication must be implemented and enforced for all access to systems, transactions, or services, including remote access and privileged access. • All access, including privileged and remote access, must be logged, and controlled. Privileged access must be monitored to detect suspicious or unauthorised behaviours.

5.	**Security Operations**	The Third Party must: • Ensure logging and monitoring is enabled for all assets to allow real-time alerting of unauthorised access or other malicious activity. • Ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support investigation and response to suspicious activities. • Ensure that appropriate malware detection and prevention tools are installed across all information technology assets used to support Medibank.
6.	**Network Management**	The Third Party must ensure that: • A network architecture must be maintained that includes, at a minimum, tiered network segmentation between: – internet accessible systems and internal systems; – systems with high security categorisations (e.g., critical systems containing personally identifiable information (PII)) and other systems; – user and server segments; and – development, test, quality assurance and production. • They use the technical capabilities (for example: multi- tenancy, or separate system landscapes) to achieve data separation among data originating from multiple customers to ensure customers shall have access only to their own data. • Restrictive configurations are implemented on all networking devices. • Firewalls are implemented to block all inbound and outbound traffic by default, only allowing authorised traffic based on the principle of least privilege.
7.	**Audit Log and Management**	The Third Party must ensure that: • They maintain complete and accurate records in relation to the scope of work, for the Term and for a period of 7 years afterwards or as directed by Medibank. • Audit logs are retained for at least one year, with a minimum of 90 days (three months) immediately available online, unless otherwise instructed. • After the completion of the retention period, audit logs are securely deleted to prevent unauthorised access or recovery
8.	**Backup & Recovery**	The Third Party must ensure that: • Information and systems used to provide services to Medibank are backed up and a backup plan is created with availability requirements. • Backups and restoration are tested regularly to confirm that recovery can be completed in a timely manner.
9.	**Configuration & Change Management**	The Third Party must ensure that: • All changes to the current configuration of assets associated with Medibank must be planned, documented, and authorised through a formal change management process. • A change request must be raised and approved before implementing any configuration changes, ensuring transparency and accountability. • After any change to the current configuration of systems associated with Medibank services: – Conduct a risk assessment following any configuration change to determine whether a security vulnerability scan is necessary.

		– If vulnerabilities are identified through a scan or other security assessment, they must be remediated promptly based on their severity and potential impact, using industry best practices.
10.	**Encryption**	The Third Party must ensure that below encryption requirements are followed: • Data in Transit Requirements - Encrypt sensitive data during transmission using secure protocols (e.g. TLS 1.2 or higher, HTTPS, VPNs, SSH). • Data at Rest Requirements - Use strong encryption (e.g. AES-256) for storing sensitive data on devices, servers, or in the cloud.
11.	**Cyber Incident Response and Business Continuity Plan**	The Third Party must ensure that: • They collaborate with Medibank to define and formalise incident response roles for all parties, including their related parties (fourth parties). • Their incident response plans align with Medibank's business continuity, crisis management, disaster recovery, and security requirements. • Their related parties (fourth parties) must regularly test and update their incident response, continuity, and recovery plans, providing Medibank with evidence of compliance and effectiveness upon request. • Cyber incident response actions are promptly communicated to Medibank and relevant internal and external stakeholders. • Appropriate supporting teams are notified immediately upon identifying an incident to ensure that incident response and recovery procedures are followed effectively and without delay. • They communicate all recovery actions taken in response to a cyber incident to Medibank and relevant stakeholders, ensuring clarity and transparency throughout the process. • They provide Medibank with a detailed incident review report after an incident impacting Medibank service has occurred. • They provide evidence of the existence, regular updates, testing, outcomes, and security of appropriate Business Continuity Management (BCM) plans. This includes detailed documentation of testing activities and results. Upon request, this information must be made available to Medibank.
12.	**Mobile Device Security**	The Third Party must ensure that: • All devices install the Medibank approved Mobile Device Management (MDM) solution to access the Medibank network and resources on mobile devices. • Users must not copy or backup Medibank data from the mobile device to any other device or removable media.

13.	**Patch and Vulnerability Management**	The Third Party must ensure that: • Systems and interfaces used for providing services to Medibank must undergo security assurance testing (e.g., vulnerability scanning, penetration test) prior to deployment in a production environment, or prior to any significant changes. • Systems or interfaces used to provide services to Medibank that are exposed on public networks must undergo at least annual penetration testing. • Security patch and vulnerability management processes are defined and implemented. • Security vulnerabilities in systems used to provide services to Medibank must be patched, updated and mitigated. • They regularly monitor approved sources for vulnerabilities, patches, and emerging threats. • Patches are tested for stability before deployment and distributed following an approved change control process.
14.	**Sanitisation Secure Disposal**	If data disposal is carried out by a third party provider, it is their responsibility to ensure that: • Verification processes are in place to confirm that data destruction has been completed effectively. • Documentation or certificates of destruction are obtained as evidence of compliance. • Records are retained and made available to Medibank upon request.
15.	**Secure Software Development**	Secure Software Development Requirements for Third Parties (Applicable for third parties who provide software development services) • Integrate security checks throughout the development lifecycle – from design to deployment. • Restrict access to source and build environments using least privilege principles. • Secure development workstations and tools based on risk. • Define and maintain secure baseline configurations for all components. • Follow industry-recognised secure coding standards and address known and emerging vulnerabilities. • Conduct manual code reviews by using independent, qualified reviewers. • Use tools such as fuzz testing and static analysis to identify input and logic flaws. • Perform regular penetration testing. • Fix all identified vulnerabilities before release to production. • Document and track security issues, fixes, and root causes to prevent recurrence. • Keep records of all code reviews, test results, and security decisions. • Provide documentation to Medibank upon request.

16.	**Information Security Management for Fourth Parties**	The Third Party must ensure that: • They regularly assess and test fourth-party security controls to ensure effectiveness and alignment with Medibank's standards. • They perform due diligence and ongoing evaluations of fourth-party security capabilities to address threats, vulnerabilities, and compliance requirements. • Regular reviews of fourth-party security control design and implementation for compliance and effectiveness are performed. • They notify Medibank promptly of any material control weaknesses in fourth parties that could impact service security, reliability, or performance. • They provide Medibank with periodic assurance that fourth-party security controls meet required standards, particularly following material changes in services. • Evidence of such assessments/evaluations, must be made available to Medibank upon request prior to signing the contract with Medibank and during the lifecycle of engagement with Medibank.
17.	**Assurance Reporting**	• Third Parties must provide a current and valid ISO 27001 certification and or SOC 2 Type 2 report to Medibank upon request, covering controls and processes related to security, availability, processing integrity, confidentiality, and privacy, as per AICPA's SOC 2 guidelines throughout the lifecycle of engagement with Medibank. • Third Parties must conduct regular independent penetration testing of their systems and networks. A comprehensive report, including findings, risk assessments, remediation actions, and identified vulnerabilities, must be provided to Medibank upon request or after significant system changes throughout the lifecycle of engagement with Medibank. • If, third party is providing payment-related services within PCI DSS scope, they must provide Medibank, upon request, with PCI DSS compliance status for services performed on their behalf and information clarifying the division of PCI DSS responsibilities, including any shared responsibilities throughout the lifecycle of engagement with Medibank.
18.	**Security Awareness**	• Third Parties must ensure all its personnel, including staff, contractors, and relevant fourth parties, receive regular information security training. Training completion must be tracked, and understanding of information security is tested periodically. • Third parties assigned Medibank accounts, must complete Medibank's mandatory compliance training within stipulated timeframes.
19.	**Information Handling**	• Use of non-Medibank devices (USBs, mobile devices, etc.) to store or transfer Medibank data is prohibited. • Email - Encrypt all email messages. Avoid attachments and use secure links to documents when possible. If attachments are necessary, password-protect them. Only share with authorised individuals and never send to personal email accounts. • Digital Records - Backup all records and ensure backups are encrypted (AES 256) at rest. • Device Restrictions - Medibank data must not be stored on personal devices. Devices containing Medibank data must be secured or attended at all times. • Confidentiality Upon Termination - The confidentiality of Medibank data must be maintained after the contractual relationship ends.

		- Cloud Storage - Unauthorised cloud storage (e.g., Google Drive, Dropbox, etc.) must not be used for storing Medibank data.
20.	**Password Management**	- Third Parties must implement robust password management practices to ensure the security of systems and sensitive data. Passwords must be strong, meeting complexity requirements, including length of characters with a combination of letters, numbers, and special characters. Passwords should be rotated and not reused. All passwords must be stored securely using encryption.
21.	**Off-Boarding Requirements for Third Parties**	The Third Party must ensure that: - They securely delete Medibank's confidential data as per regulatory and contractual compliance. - They return all documents related to the engagement to Medibank based on request. - They remove all physical and logical access for personnel supporting Medibank work and confirm if all accesses (physical and logical) have been revoked.

5. CONSEQUENCES OF NON-COMPLIANCE

Non-compliance with this standard may result in contract termination, penalties, or other remedial actions.

6. DEFINITIONS

This table defines the terms used throughout this standard.

Term	Definition
Related Party/Parties	An entity, organisation or individual that has a direct or indirect relationship with the Third Party and plays a role in delivering services or operations to Medibank.
Service Provider/Providers	Any third-party organisation that provides services or support to Medibank under a contractual agreement.
Third Party/Parties	An external entity engaged by Medibank to deliver services to Medibank.
Fourth Party/Parties	A subcontractor/s or related party engaged by the third party to deliver services to Medibank.
Incident Response Plan	A structured approach outlining processes to detect, respond to, and recover from security incidents.
Penetration Testing	A simulated attack on systems or networks to identify vulnerabilities and test the effectiveness of security controls.
SOC 2 Type 2 Report	An independent report assessing a third party's controls for security.
PCI DSS	The Payment Card Industry Data Security Standard, which establishes security requirements for protecting cardholder data.
CPS 234	Prudential Standard CPS 234 (Information Security) issued by APRA establishes minimum information security requirements for regulated entities.
Remediation Plan	A documented strategy to address identified security gaps or weaknesses, including timelines and actions.
Material Control Weakness	A material control weakness refers to a significant deficiency or failure in a control or set of controls that creates a substantial risk of non-compliance, operational disruption, or security compromise.