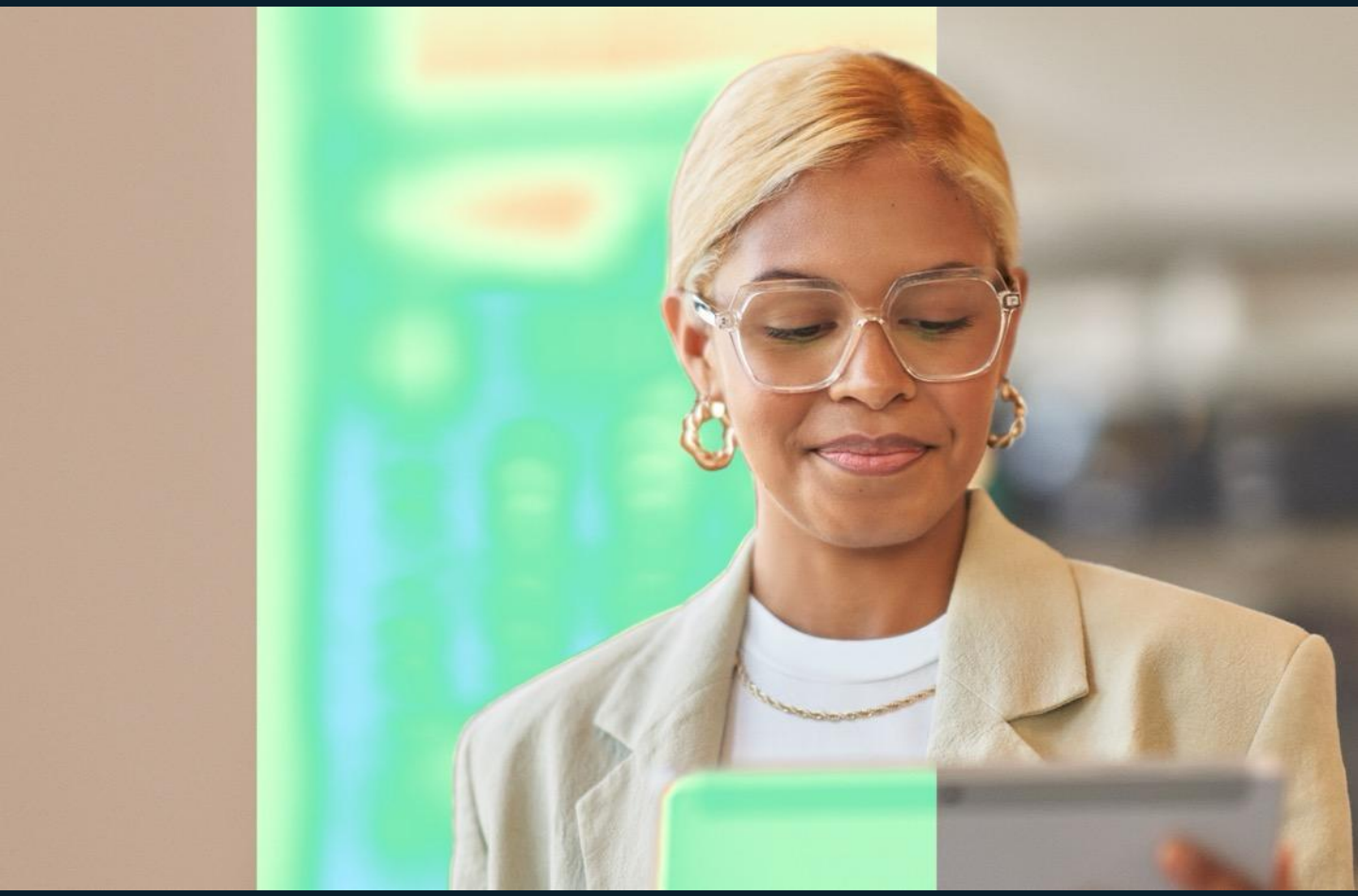
SMB Security Regulatory Changes: What your business needs to know



From 2025, the Australian government is proposing two key regulatory changes that will impact small and medium businesses (SMBs):

a. Removal of the small business exemption from the Privacy Act
b. The rise of industry-led cybersecurity frameworks like SMB1001

With millions of SMBs potentially impacted, businesses must take proactive steps to comply. Failure to do so could lead to significant penalties if there is a breach.

Additionally, these security controls align closely with requirements for responsible AI adoption, turning compliance investments into strategic assets for future business growth.

Privacy Act amendment: Removal of small business exemption

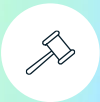
The Privacy Act 1988 applies to most Australian businesses, requiring them to handle personal information in accordance with strict guidelines. However, SMBs with an annual turnover of less than $3 million have been generally exempt unless they fall into specific categories like health service providers or those trading in personal information.

If legislated, this exemption will be removed, with implementation expected to begin in 2025 and include a transition period to allow businesses time to adapt.

Requirements for all businesses

To comply with the Privacy Act, all businesses regardless of size or turnover, need to:

1. **Develop and maintain a privacy policy** that explains how you collect, use, disclose and protect personal information.
2. **Implement the Australian Privacy Principles (APPs)** including:
   a. Only collecting personal information that's necessary for your functions
   b. Providing clear information about why you're collecting data
   c. Securing personal information against misuse, loss and unauthorised access
   d. Allowing individuals to access and correct their personal information
   e. Using information only for the purpose it was collected
3. **Create a data breach response plan** to detect, contain, assess and notify individuals affected by eligible data breaches (those likely to result in serious harm).
4. **Apply privacy by design** principles to new processes, products and services that involve personal information.



Penalties for non-compliance

If there is a breach, the potential maximum penalties for Privacy Act violations could include:

- Up to $50 million for serious or repeated privacy breaches
- Three times the value of any benefit obtained through the misuse of information
- 30% of a company's adjusted turnover during the relevant period

SMB1001 Cybersecurity Compliance Framework

SMB1001 is a cybersecurity framework specifically designed for small and medium businesses. Published in 2024, this framework provides a structured approach to achieving cybersecurity certification.

It introduces a tiered certification model (Bronze, Silver, Gold) to help SMBs strengthen their cybersecurity posture. Bronze establishes essential foundations, Silver adds comprehensive controls, and Gold represents advanced security maturity for handling sensitive data.

While not government-mandated, SMB1001 is an industry-led framework that incorporates elements from established standards like the Essential Eight and ISO 27001, but is specifically designed to be more accessible and practical for smaller businesses.

Key components of the framework

Governance Controls

a. Establishing security roles and responsibilities
b. Implementing security policies and procedures
c. Regular security risk assessments
d. Incident response planning

Technical Controls

a. Identity and access management requirements
b. Data protection and encryption standards
c. Network security and monitoring
d. Endpoint protection requirements
e. Backup and recovery protocols

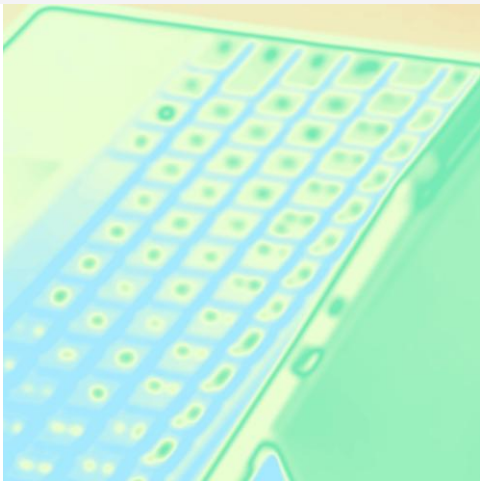
Operational Controls

a. Security awareness training for all staff
b. Third-party vendor risk management
c. Change management procedures
d. Regular security testing and validation

Compliance timeline and approach

While full details of the certification process are still being finalised, businesses should prepare by:

- **Conducting a gap assessment** against the framework requirements
- **Developing a remediation roadmap** to address identified gaps
- **Implementing required controls** in a prioritised manner
- **Documenting evidence of compliance** for certification purposes
- **Preparing for regular reassessment** as the framework evolves



Business impact and strategic considerations

These regulatory changes represent both a challenge and an opportunity for small and medium businesses:

Business challenges

- Additional compliance costs and resource requirements
- Need for specialised security and privacy expertise
- Potential operational changes to meet new requirements

Strategic opportunities

- Enhanced trust with customers and partners through demonstrated compliance
- Reduced risk of costly security incidents and data breaches
- Competitive advantage in an increasingly security-conscious market
- Better positioning for contracts with larger organisations and government entities

Getting prepared: A practical approach

Rather than viewing these changes as purely compliance hurdles, forward-thinking businesses are using them as catalysts to improve their overall security posture:

- **Start early:** Begin compliance efforts now to avoid a last-minute rush
- **Take a risk-based approach:** Focus first on your most sensitive data and critical systems
- **Leverage integrated solutions:** Use platforms like Microsoft 365 that address multiple compliance requirements
- **Document everything:** Maintain precise records of your compliance efforts and security controls
- **Seek expert guidance:** Work with a qualified technology partner who understands both the regulatory requirements and practical implementation

By proactively addressing these upcoming regulatory changes, your business can not only meet compliance requirements but also build a stronger security foundation that protects your most valuable assets and supports sustainable growth.

DICKER DATA | Microsoft

About Dicker Data

As Australia's largest owned and operated technology distributor, we represent over 8,000 technology providers. We've created a network of specialist cyber security partners who help Australian healthcare organisations mitigate risks and defend against increasing threats.

Meet our proven healthcare security partners

CUBESYS

cubesys is a Microsoft Partner helping healthcare organisations modernise with Azure, Microsoft 365, automation and managed services. We deliver secure, scalable solutions that support compliance, protect data and improve workflows. We work closely with our customers to ensure fast, effective, and secure outcomes. Learn more at cubesys.com.au or email sales@cubesys.com.au.

daraco I.T. SERVICES

Daraco IT, a leader in technology services and Cyber Security, exceling in safeguarding digital landscapes. With a mission to empower healthcare providers through cutting-edge technologies and expert strategies, we provide robust protection against cyber threats, fostering secure and resilient environments for our clients. Learn more at www.daraco.com.au/health-solutions or call 1300 327 226

Spirit

Spirit delivers secure, scalable ICT solutions tailored for the unique and evolving needs of the healthcare sector. We support our clients to boost productivity, achieve seamless connectivity and ease the administrative burden. Spirit empowers healthcare teams with reliable solutions that keep operations secure and efficient. Learn more at spirit.com.au or email spirit@spirit.com.au.

Connect with a proven healthcare security specialist:
dickerdata.com.au/microsoft/healthcare-security