

Cybersecurity Uplift SMB1001 Program Grants 2026 Expression of Interest Guidelines

Hunter New England Central Coast Primary Health Network (PHN) recognises small to medium sized businesses are increasingly targets of cyber threats due to limited resources and potentially immature security controls.

To support small and medium sized Allied Health Practices and General Practices, the PHN are making available ten (10) grants via the Cybersecurity Uplift SMB1001 Program Grant round. This initiative is targeted towards practice owners or IT Managers who agree to work with the PHN's consultant and are willing to financially invest in their business to uplift their digital security.

Practices will work with a cybersecurity consultant to support implementation of a **security framework** specifically designed to protect small to medium businesses. The **framework** known as **SMB1001**, developed by Dynamic Standards International (DSI), offers a practical cybersecurity framework providing a clear pathway to improve cyber maturity without overburdening small to medium-size business owners.

The SMB1001 Cybersecurity Uplift Program supports participating businesses to achieve Tier 2 alignment across technical controls, governance, policies, processes and staff awareness. A cybersecurity technical consultant will assess the Practice's technology environment, identify gaps and implement approved, in-scope security improvements at no cost to the Practice. These improvements may include multi-factor authentication, firewall configuration, password management, secure backups, access controls, patching and related security measures. The program also provides policies, resources and an implementation plan to improve cybersecurity maturity, reduce third-party risk and support applicable Australian privacy obligations.

Tier 2 alignment reduces risk but cannot prevent every cyberattack or eliminate all cybersecurity risks. The Practice remains responsible for maintaining implemented controls, managing service providers and addressing ongoing risks after the program.

The grant will provide a package of pre-paid consulting hours to support implementation of recommended changes to meet the standard. A **co-payment of \$200 ex GST** will be required as a commitment to participation. The \$200 will be used towards one additional hour of IT support with the consultant engaged for this initiative.

Cybersecurity Uplift Program Support Package

The Cybersecurity Uplift Program supports participating Practices to achieve alignment with Tier 2 of the SMB1001 Cybersecurity Standard. The program takes a whole-of-business approach to assessing the Practice's current cybersecurity position. The assessment may cover:

- Staff and administrator accounts
- Computers, laptops and other devices
- Email systems and security settings
- Websites and internet connections
- Firewalls and security software
- Multi-factor authentication
- Password management
- Software updates and patching
- Data backups and restoration
- Access controls
- Payment and invoice processes
- Confidentiality arrangements
- IT service arrangements

- Physical security and visitor management
- Relevant policies, procedures and records

As a condition of participation, the Practice must provide the cybersecurity consultant with accurate information and authorised access needed to complete the assessment and approved uplift work. The Practice's existing IT provider may be asked to:

- Provide relevant technical information
- Explain the current technology environment
- Supply system and configuration details
- Provide authorised access where required
- Support safe access to systems under its management
- Confirm dependencies that may affect the proposed work

The existing IT provider is not responsible for conducting the SMB1001 assessment or delivering the funded cybersecurity uplift. The cybersecurity consultant will assess the environment, define the required improvements and implement approved activities within the program scope.

The assessment and uplift process will generally **take one to two months**. Timing will depend on the Practice's size, existing environment, availability and technical requirements. The program is scheduled to **commence in October 2026**.

Tier 2 technical uplift

Following the assessment, the cybersecurity consultant will prepare an implementation plan. The plan will identify existing strengths, security gaps, priorities and actions required to support SMB1001 Tier 2 alignment.

The consultant will explain the proposed changes and obtain appropriate authorisation before implementation. Approved, in-scope uplift activities will be completed by the cybersecurity consultant at no cost to the Practice.

The program focuses on practical improvements within the Practice's existing technology environment. It does not include replacing the entire environment.

Any major hardware replacement, new commercial software subscription or material system change outside the approved scope will be documented and discussed with the Practice. These items will not proceed without the Practice's specific approval. Any associated costs will remain the Practice's responsibility.

Funded support package

Successful applicants will receive a support package valued at \$10,000 excluding GST. The package includes:

- Program onboarding and administration
- A mandatory virtual education session of approximately one hour
- A whole-of-business cybersecurity maturity assessment
- An assessment against SMB1001 Tier 2 requirements
- Identification of existing strengths, weaknesses, risks and priorities
- A defined remediation and uplift plan
- Technical assessment by the cybersecurity consultant
- Implementation of approved, in-scope technical security improvements
- Liaison with the existing IT provider for information and authorised access
- Governance templates, guides and supporting resources
- Practical guidance for implementing operational and governance changes
- Review and validation of completed uplift activities
- A record of completed work and any remaining actions

Items not included

The program does not include:

- General IT support unrelated to the approved uplift
- Work outside the agreed SMB1001 Tier 2 scope
- Major equipment or system replacement
- Commercial subscriptions or licence costs outside the funded package
- Ongoing management of the Practice's IT environment
- Emergency cyber incident response, forensic investigation or breach recovery
- Remediation of unrelated operational or technical issues
- Work required because information or access was not provided when requested

Practice responsibilities

The Practice must:

- Provide accurate and complete information
- Provide authorised access needed for the assessment and uplift
- Support reasonable coordination with its existing IT provider
- Review and approve proposed technical changes
- Participate in required education and consultation activities
- Maintain the controls implemented through the program
- Manage ongoing subscriptions, licences and service arrangements
- Address any work identified outside the funded scope
- Maintain suitable IT support after the program concludes

The program is designed to improve cybersecurity maturity and support SMB1001 Tier 2 alignment. It reduces cybersecurity risk but cannot prevent every cyberattack or remove all business risk. The Practice remains responsible for maintaining its systems, controls, service providers and ongoing cybersecurity arrangements.

Potential Practice Costs

The program funds the cybersecurity assessment, remediation planning and implementation of approved technical uplift activities within the agreed program scope. The cybersecurity consultant will complete this work at no cost to the Practice.

The Practice may need to fund products, licences, equipment, subscriptions, major migrations or work outside the approved scope. The consultant will explain any proposed cost before the Practice makes a commitment.

Where an approved control can be implemented within the existing environment, the cybersecurity consultant's installation and configuration work will form part of the funded program. The Practice remains responsible for approving and paying for any required third-party products, licences, equipment or services.

Eligibility and Selection Criteria

Applicants will be assessed against the minimum eligibility requirements and the quality of their EOI responses. A further screening assessment may be completed before acceptance. This assessment will confirm the Practice's technical suitability, readiness, available access and ability to participate in the program. Participating Practices must:

- Nominate a project contact and an authorised decision-maker.
- Attend agreed online meetings, education sessions and program check-ins.
- Provide accurate information about their business, systems and service providers through approved secure methods.

- Provide the cybersecurity consultant with authorised access required to complete the assessment and approved uplift activities.
- Authorise their existing IT provider to supply relevant technical information and provide access where required.
- Ensure that temporary access is removed after the approved work is completed.
- Review and approve proposed changes before implementation.
- Complete all required program evaluations, including the final survey issued four weeks after the implementation period.
- Maintain implemented controls and ongoing service arrangements after the program concludes.

The existing IT provider is not responsible for conducting the SMB1001 assessment or delivering the funded technical uplift. Their role is limited to providing relevant information, explaining the existing environment and facilitating authorised access for the cybersecurity consultant.

Applicants must demonstrate that the Practice:

- Operates and delivers services within the Hunter New England and Central Coast region.
- Has the support of the Practice owner or authorised decision-maker.
- Is ready to engage with the cybersecurity consultant.
- Is willing to participate in required education and consultation activities.
- Can provide the information and access needed to complete the work.
- Is willing to consider and fund approved products, licences, equipment or services that fall outside the funded package.
- Can maintain implemented controls following completion of the program.

Where **Microsoft 365 Business Premium**, or another approved service, is required for program compatibility, the requirement must be confirmed during commencement. The Practice will be advised before acceptance if it must obtain or upgrade licensing at its own cost.

Terms & Conditions

The following PHN terms and conditions will apply:

- The Expression of Interest (EOI) must be submitted by the applicant (owner or IT Manager or person responsible for IT).
- All conflicts of interest are to be declared.
- The PHN will not directly reimburse any associated costs including wages involved in completing the training, costs involved in undertaking the implementation and uplift, purchase of required IT equipment and systems, or ongoing compliance costs.
- An EOI does not guarantee a grant. Assessment of EOI's will be based on meeting the criteria and responses to the questions in the EOI. Successful applicants will be notified.
- Applicants must agree for their details to be supplied to the consultant to allow contact to carry out the grant activities.
- Applicants from Practices who intend on closing within the next 12 months or from applicants who are not intending to remain in the employment or ownership of the organisation for the next 12 months are ineligible.
- Successful applicants will sign a Letter of Agreement to acknowledge the terms and conditions of the grant.
- Applicants must have a valid ABN number.
- Applicants can only submit one (1) application per ABN (including multi-site providers)
- HNECC PHN Terms and Conditions will apply.
- Applications that do not meet the criteria will not be eligible.
- Applicants are to notify the PHN immediately and prior to any training or consultation if circumstances have changed and they are unable to complete the requirements.
- NSW Health (LHD) practices are ineligible to apply.

Ineligible:

Previous grant recipients are eligible only if they have fully complied with any previous PHN funding contract commitments including performance, reporting and acquittal requirements.

Expression of Interest (EOI) Process:

General Practices (including Aboriginal Community Controlled Health Organisations) and Allied Health Practices are invited to complete an Expression of Interest, via SmartyGrants.

The PHN reserves the right to extend the advertised closing date of the EOI based on the number of applications received.

Applications will be assessed against the criteria and as deemed by the subject matter experts within the PHN.

Applicants will be contacted to discuss their eligibility and ability to meet the criteria. This includes completing a technical compliance survey. This will constitute part of the assessment.

For more information contact:

Contact grants@thephn.com.au