

Cyber Invest Business Program Guidelines

Department of Corporate and Digital Development

This grant is administered by the Department of Trade, Business and Asian Relations on behalf of the Department of Corporate and Digital Development.



Document title	Cyber Invest Business Program Guidelines
Contact details	Cyber Resilience, DCDD
Approved by	Chief Executive, DCDD
Date approved	29/09/2026
Document review	After each grant round (twice per year)

Version	Date	Author	Changes made
0.1	20/8/2026	DTBAR Grants Delivery & Systems	First draft
0.2	16/09/2026	DTBAR Grants Delivery & Systems DCDD Cyber Resilience	Updated to include changes for Round 2
1.0	29/09/2026	DTBAR Grants Delivery & Systems DCDD Cyber Resilience	Approved version

Acronyms	Full form
ABN	Australian Business Number
ACSC	Australian Cyber Security Centre
CE	Chief Executive
DCDD	Department of Corporate and Digital Development
DTBAR	Department of Trade, Business and Asian Relations
ICT	Information and Communication Technology
NTG	Northern Territory Government

Contents

1. Purpose.....	4
1.1. Objectives.....	4
2. Program governance.....	4
3. Funding conditions.....	4
4. Eligibility requirements	5
4.1. Eligibility criteria – applicants	5
4.2. Eligibility criteria – funded activity	5
4.3. Excluded entities	5
4.4. Excluded expenditure.....	5
5. Support categories	6
5.1. Cyber Foundations.....	6
5.2. Cloud Security.....	6
5.3. Essential Eight Uplift	7
5.4. Managed Cyber Security Service	7
6. Application process.....	8
6.1. Before you apply	8
6.2. How to apply.....	8
7. Assessment process.....	9
7.1. Assessment criteria.....	9
8. Funding decision.....	9
8.1. Funding decisions.....	9
8.2. Notification of outcome.....	9
9. Contract arrangement (agreement).....	10
9.1. Payment	10
9.1.1. First payment.....	10
9.1.2. Final payment	10
9.2. Variations	10
10. Contacts	10
11. Appendix A – Eligible activities: Cyber Foundations	11
12. Appendix B - Eligible activities: Cloud Security	12
13. Appendix C – Eligible activities: Essential Eight Uplift.....	13
14. Appendix D – Eligible activities: Managed Cyber Security Service.....	14

1. Purpose

The Cyber Invest Business Program (the program) is a Northern Territory Government (NTG) initiative to support small to medium Territory businesses to improve their cyber security and resilience to protect against common cyber security threats and their impacts.

This program is administered by the Department of Trade, Business and Asian Relations (DTBAR) on behalf of the Department of Corporate and Digital Development (DCDD).

1.1. Objectives

The program objectives are:

- Support businesses to enhance their protection and resilience against cyber security threats.
- Reduce the risk of compromise to business systems and data.
- Avoid business disruption and reputational damage that can result from cyberattacks.
- Increase demand for specialised cyber security services delivered by Territory Enterprises, supporting local industry capability and cyber security jobs.

2. Program governance

The DTBAR General Grant Terms and Conditions apply to this program and form part of these Program Guidelines, unless expressly varied or replaced by provisions contained within these Program Guidelines.

In the event of any inconsistency between the General Grant Terms and Conditions and these Program Guidelines, the provisions of these Program Guidelines will prevail to the extent of the inconsistency.

DTBAR reserves the right to amend or update the General Grant Terms and Conditions from time to time, as required.

3. Funding conditions

- The program opens twice each financial year.
- Opening and closing dates for each round will be published on the GrantsNT website.
- Applications cannot be submitted after a round has closed.
- Funding is on a first come first served basis until all available funds have been allocated or the funding round closes, whichever may occur first.
- The grant will fund up to 50% of eligible project costs, to a maximum grant of \$20,000 per business per financial year. The applicant must fund the remaining eligible project costs and any ineligible or additional costs.
- Successful applicants must complete the implementation component of the project and all reporting requirements within four months of the funding agreement being issued. Approved software subscriptions and managed services may continue for the approved funding period, up to a maximum of 24 months.
- Multiple applications may be submitted provided the total grant funding approved for the business does not exceed \$20,000 in a financial year.

4. Eligibility requirements

4.1. Eligibility criteria – applicants

To be eligible, the applicant must demonstrate they meet all the following:

- Be a Territory Enterprise.
- Active Australian Business Number (ABN).
- A legal entity (for-profit or not-for-profit).
- Have a turnover of less than \$10 million.

4.2. Eligibility criteria – funded activity

Applicants can apply for funding for a cyber security project aligned to one or more of the support categories listed in section 5 below. Funding may be used for items below, where directly related to an approved project. Detailed eligible activities are contained in Appendices A-D:

- a. Professional services
- b. Software licences and subscriptions (up to 24 months)
- c. Hardware explicitly listed in the Appendices
- d. Managed cyber security service (up to 24 months)

4.3. Excluded entities

The following applicants are not eligible to apply:

- a. Private and public educational institutions, government agencies and government owned bodies, statutory corporations and local government bodies.
- b. Publicly listed companies.
- c. Applicants that have already received the maximum funding available under the Cyber Invest Business Program in the financial year that they applied.

4.4. Excluded expenditure

The program is unable to support:

- a. Projects or costs that have already been funded
- b. Renewals of existing subscriptions or managed services
- c. Subscriptions or managed services beyond the approved maximum period (24 months)
- d. Expenditure incurred before approval
- e. Costs funded by another government program
- f. Hardware not explicitly listed as eligible in the relevant appendix
- g. Internet connectivity
- h. General cloud migration that does not explicitly include secure configuration

- i. Website design, hosting and non-security development
- j. General ICT support
- k. Cyber security reviews, assessments, penetration tests or audits that are not explicitly required for an uplift project
- l. Accreditation, certification and membership fees
- m. Cyber insurance
- n. Travel and accommodation
- o. Physical security
- p. Incident-response costs relating to an existing or recent attack.

5. Support categories

Businesses must design a cyber security project aligned to one or more of the categories listed below.

5.1. Cyber Foundations

A project to implement the essential cyber security protections recommended in the Australian Cyber Security Centre (ACSC) [Small Business Cyber Security Guide](#)¹ and [Checklist](#).² This category is suitable for businesses who are not sure where to start and want to get basic protections in place.

Businesses are encouraged to complete the free ACSC [Cyber Health Check](#)³ to help identify their cyber security needs before designing a project. Businesses can also work with a local ICT or cyber security firm to design a project.

Details of eligible costs are provided in Appendix A.

5.2. Cloud Security

A project to securely configure Microsoft 365 or ChromeOS cloud services in line with the ACSC [Small Business Cloud Security Guides](#).⁴ These ACSC guides adapt Essential Eight principles to cloud environments and focus on practical security controls for small businesses. This category is suitable for businesses that are looking to secure their cloud services.

A Microsoft 365 project must use eligible software licensing that supports the security controls being implemented. Eligible licensing is specified in Appendix B. Funding may support a new subscription or an upgrade from an eligible lower-tier subscription for up to 24 months. Businesses will need to be able to fund licensing ongoing after the grant.

The project may include up to 24 months of managed cloud service from a local NT cyber security or ICT firm; however, this is not mandatory. The business can elect for a project to obtain support to initially configure the environment securely and then self-manage the environment ongoing to keep costs down. If the business elects to use a managed service, the business must be able to fund ongoing management costs after the initial 24 months.

Details of eligible costs are provided in Appendix B.

¹ <https://www.cyber.gov.au/business-government/small-business-cyber-security/small-business-hub/small-business-cyber-security-guide>

² <https://www.cyber.gov.au/sites/default/files/2025-03/Small%20business%20cyber%20security%20checklist%20%28June%202023%29.pdf>

³ <https://www.cyber.gov.au/cyberhealthcheck>

⁴ <https://www.cyber.gov.au/business-government/small-business-cyber-security/small-business-hub/small-business-cloud-security-guides>

5.3. Essential Eight Uplift

A project to implement or improve cyber security controls aligned with the [ACSC Essential Eight](#)⁵ framework.⁶ This category is suitable for businesses who have already implemented the basic cyber security measures described in section 5.1 Cyber Foundations and are ready to undertake a more structured or technically complex security uplift. This category is suitable for businesses that:

- have more complex systems or heightened cyber risks;
- need to meet customer, contractual or supply-chain expectations; or
- are ready to work towards a defined Essential Eight maturity level.

Projects may implement or improve one or more Essential Eight mitigation strategies; or work towards a nominated Essential Eight maturity level across all eight mitigation strategies.

The application and quote must identify:

- the Essential Eight mitigation strategy or strategies being addressed
- the controls that will be implemented or improved
- the products and professional services required
- any ongoing costs the business must meet after grant funding ends.

Details of eligible costs are provided in Appendix C.

5.4. Managed Cyber Security Service

A project to commence a managed cyber security service or add new, separately priced cyber security capabilities to an existing managed ICT arrangement. Funding for an approved managed cyber security service is available once, for a maximum of 24 months.

Quotes must be itemised and separate out managed cyber security services from general ICT support managed services. Businesses must be able to fund the security services after the end of the funded period. The grant funding is intended for businesses to be pro-active and is not available to assist with a current or recent attack that has already occurred.

A managed cyber security service is an ongoing service where cyber security specialist personnel actively monitor, investigate, manage or respond to cyber security events. This may include remediating vulnerabilities and implementing security controls on behalf of the applicant. The managed security service must include documented investigation, escalation and response arrangements.

Consultancy, advisory or reporting services on their own do not constitute a managed cyber security service.

Access to software, dashboards, portals, reporting tools, scanning tools, assessment tools or automated security platforms does not, by itself, constitute a managed cyber security service. The primary purpose of the funded service must be ongoing managed cyber security services delivered by people, rather than access to software, platforms or automated tooling. Funding may be approved for relevant software and

⁵ <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight>

⁶ The program may be updated to reflect changes to Australian Government cyber security frameworks and guidance.

subscriptions for up to 24 months, if this software is explicitly required for the managed cyber security service.

The application and quote must identify:

- security services included
- software or subscriptions included
- documented support arrangements, including responsibilities of the applicant and provider
- any ongoing costs the business must meet after grant funding ends

Details of eligible costs are provided in Appendix D.

6. Application process

6.1. Before you apply

- Read the Cyber Invest Business Program Guidelines (this document)
- Read the [General Terms and Conditions – Grants and Subsidies \(pdf\)](#)⁷
- Complete the free ACSC [Cyber Health Check](#)⁸ to help determine your cyber security needs.
- Choose an ICT or cyber security provider:

The Northern Territory Government does not approve, endorse or accredit providers under this program. Before selecting a cyber security or ICT firm, review the guidance published on the [CyberNT](#)⁹ website. Applicants are responsible for undertaking appropriate due diligence before engaging a provider. You **must** select a provider that is a [Territory Enterprise](#).¹⁰

- Prepare your supporting materials:
 - Description of the project
 - Itemised quote

6.2. How to apply

You must apply on the [GrantsNT](#) website. Further information about the Application Process is in the [General Terms and Conditions – Grants and Subsidies \(pdf\)](#).

You must provide an itemised quote that meets the requirements of the selected support category.

You must provide a description of your project including:

- relevant support category or categories
- proposed activities
- products, subscriptions or services required for the project

⁷ https://nt.gov.au/__data/assets/pdf_file/0007/1620556/General-Terms-and-Conditions-Grants-and-Subsidies.pdf

⁸ <https://www.cyber.gov.au/cyberhealthcheck>

⁹ <https://cyber.nt.gov.au/cyber-invest-business-program/grant-applicants>

¹⁰ See definition of Territory Enterprise in the General Terms and Conditions

- project timeframe (maximum of 4 months)
- ongoing subscription or service costs the business will need to meet after the grant funding ends

7. Assessment process

Applications will be assessed and managed by the Grants, Delivery and Systems team within DTBAR on a first come first served basis. Incomplete applications will not be assessed.

7.1. Assessment criteria

What we are assessing	What we are looking for
Project eligibility	Alignment with one or more support category
Cyber security uplift	The project implements one or more cyber security controls identified in the selected support category.
Scope of works	Specific deliverables
Value for money	Reasonable and itemised costs
Provider eligibility	Professional or managed services are supplied by an eligible Territory Enterprise that provides ICT or cyber security services.
Managed service suitability	Service involves ongoing human monitoring, investigation or response rather than primarily software access.
Sustainability	The business understands and can fund ongoing subscription, licence or service costs after grant funding ends.

8. Funding decision

8.1. Funding decisions

The funding decision is made by the DCDD delegate. Decisions are final. The delegate may:

- Approve funding
- Approve funding subject to conditions
- Decline funding

The fact that an applicant has met eligibility requirements does not guarantee funding.

8.2. Notification of outcome

All applicants will receive written notification of the outcome of their application. Where an application is declined, DTBAR reserves the right to limit feedback to the relevant eligibility or assessment requirement that was not met. DTBAR is not required to provide detailed reasons or commentary on the assessment.

The decision to decline an application is final. Where the program round remains open, an applicant may submit a new application that addresses the relevant requirements. Applicants may also apply in a future round, where relevant and appropriate.

9. Contract arrangement (agreement)

Successful applicants will be required to enter into a legally binding funding agreement with the Northern Territory Government. The purpose of the funding agreement is to establish the obligation of the parties, including, but not limited to the mandatory reporting requirements, including required evidence, due dates and other relevant conditions, as set out in the funding agreement.

Applicants who receive a funding offer will need to **accept or request changes to the offer within 5 business days** from notification. DCDD reserves the right to decide to continue funding or accept changes for an applicant who has let the time limit lapse.

9.1. Payment

9.1.1. First payment

An initial payment of 50% of the total funding amount approved will be paid on execution of a signed funding agreement.

Note: The DCDD delegate has the discretion to change the upfront percentage payment if negotiated before the agreement is signed by the applicant.

9.1.2. Final payment

The final 50% payment will be paid on the applicant completing their reporting requirements to DCDD's satisfaction.

9.2. Variations

Variations can only be for the purposes of changes to the scope of works, including using a different supplier. Applicants may make a request to vary a funding agreement by making a written request via their application in GrantsNT.

10. Contacts

Grants Administration Contact

Grants, Delivery and Systems, DTBAR

Email: Business.Programs@nt.gov.au

Ph: 08 8999 6902

<https://grantsnt.nt.gov.au/>

Program Contact

Cyber Resilience Business Unit, DCDD

Email: Cyber.Invest@nt.gov.au

Ph: 08 8999 3845

<https://cyber.nt.gov.au/>

11. Appendix A – Eligible activities: Cyber Foundations

A project to implement the essential cyber security protections recommended in the [ACSC Small Business Cyber Security Guide](#) and [Checklist](#)

Item	Eligible	Not eligible	Notes
Professional services	- Set up multi-factor authentication. - Set up a password manager. - Configure accounts to require strong passphrases. - Replace shared accounts with individual user accounts. - Configure role-based user access. - Configure automatic device and software updates. - Configure built-in antivirus software to conduct regular scans of devices (e.g. Windows Security). - Create a backup plan (either external device or cloud). - Configure automatic backups. - Set up an external storage device for backups. - Configure security settings on existing servers, internet-facing services, and network devices (e.g. routers). - Configure security controls for an existing business website, such as MFA for administrator access, security updates and backups. - Securely erase and factory reset devices before disposal, sale or reuse. - Configure devices to automatically lock after a short time of inactivity. - Deliver basic cyber awareness training using recognised resources (e.g. free resources from ACSC or Cyber Wardens). - Prepare a practical cyber incident emergency plan and explain how to use it.	- Assessments, scans or reports that do not include implementation of controls or improvement in security. - General cloud migration that does not explicitly include secure configuration. - Website hosting, redesign or general development. - General IT support or equipment replacement.	- Quote must identify each control to be configured or implemented. - Supplier must provide clear handover instructions to the business.
Software or subscriptions	- Password manager software or subscription (up to 24 months). - Cloud backup storage subscription (up to 24 months).	- Operating systems. - General cloud storage not used for backups. - General business software. - Renewals of existing or previously funded subscriptions.	- Software subscriptions are one-off support only. - Businesses must be able to maintain the subscription after the initial 24 months.
Hardware	- Multi-factor authentication security keys or hardware tokens (e.g. YubiKeys). - External backup storage device (e.g. external hard drive, NAS device).	- Mobile phones, tablets, computers, laptops. - Servers. - Network devices. - Printers/multifunction devices. - General ICT infrastructure upgrades.	- Hardware must be new, itemised and necessary for the approved control. - Backup devices must be dedicated to backup and configured as part of the project.

12. Appendix B - Eligible activities: Cloud Security

A project to securely configure Microsoft 365 or ChromeOS cloud services in line with the relevant [ACSC Small Business Cloud Security Guides](#).

	Eligible	Not eligible	Notes
Professional and managed services	• Enable security defaults in the Microsoft 365 or ChromeOS cloud environment. • Configure Microsoft 365 security controls (follow or adapt the technical examples in the ACSC guides). • Configure ChromeOS security controls using the ACSC guide. • Enrol existing devices in Mobile Device Management (Intune or Google). • Provide configuration records and administrator handover instructions. • Provide up to 24 months of managed cloud service for the newly configured environment.	• Assessments, review, scanning or testing of environment that does not include improving security. • General migration to Microsoft 365, Google Workspace or other cloud services without security configuration. • Cloud migration or data migration where the primary purpose of the project is business transformation, system replacement or productivity improvement rather than cyber security uplift. • General IT support. • Renewal of existing managed cloud service.	• Quote must identify the guide-aligned settings to be configured. • Applicant may choose initial configuration only and self-manage the cloud environment ongoing. • The managed cloud service component is optional. • Funding for the managed cloud service is available once, for a maximum of 24 months, and cannot be renewed through a future grant. • Businesses must be able to maintain the ongoing costs of the managed cloud service.
Software or subscriptions	• Microsoft 365 Business Premium (up to 24 months). • Upgrade from Microsoft 365 Business Basic or Standard to Microsoft 365 Business Premium (up to 24 months). • Microsoft Entra ID P2 licenses (referred to as Azure Active Directory Premium P2 in the ACSC guide) for administrators (up to 24 months). • Equivalent Chromebook or ChromeOS security licensing (up to 24 months).	• Renewal of existing Business Premium subscription. • Renewal of software obtained under previous grant application. • General productivity licensing not required for approved security controls.	• Software subscriptions are available as a one-off and cannot be applied for in subsequent grant applications. • Grant funding can be used if a business is upgrading from a lower Microsoft subscription (basic or standard) but not for renewing Business Premium. • Businesses must be able to maintain ongoing licensing requirements. • The Entra ID P2 license is only required for a limited number of administrators.
Hardware	• N/A.	• All hardware and equipment.	• No hardware is funded under this category.

13. Appendix C – Eligible activities: Essential Eight Uplift

A project to implement or improve cyber security controls aligned with the [ACSC Essential Eight](#) framework.

	Eligible	Not eligible	Notes
Professional services	- Professional services to implement or improve an Essential Eight control. - Configuration of existing systems and equipment. - A baseline review where it is conducted as part of the implementation project. - Remediation of control gaps identified during the project. - Testing that confirms the funded controls have been implemented and operate as intended. - Policies, procedures and documentation directly required to operate an implemented control. - Training required to support the implemented control.	- An Essential Eight assessment, maturity review, report or gap analysis on its own, that does not include control implementation. - General IT support. - General digital transformation or replacement of business systems. - Generic policy or procedure packs. - Certification or accreditation. - Costs primarily associated with cyber security measures outside the Essential Eight. - Penetration testing or vulnerability assessments unrelated to validating funded controls.	- A project is not required to achieve an overall Essential Eight Maturity Level. - The quote should identify how each quoted product, licence, hardware item or service contributes to the identified Essential Eight control.
Software or subscriptions	Security software or subscription required to implement and/or maintain an identified control (up to 24 months).	- Software or subscriptions that are not mapped to an identified Essential Eight control. - Renewals of existing or previously funded software or subscriptions.	
Hardware	- Multi-factor authentication security keys or hardware tokens (e.g. YubiKeys). - External backup storage device (e.g. external hard drive, NAS device).	- Mobile phones, tablets, computers, laptops. - Servers. - Network devices. - Printers/multifunction devices. - General ICT infrastructure upgrades.	- Hardware must be new, itemised and necessary for the approved control. - Backup devices must be dedicated to backup and configured as part of the project.

14. Appendix D – Eligible activities: Managed Cyber Security Service

A project to commence a managed cyber security service or add new, separately priced cyber security capabilities to an existing managed ICT arrangement.

	Eligible	Not eligible	Notes
Professional and managed services	- Initial onboarding and secure configuration required to commence the managed security service. - A new separately priced security capability can be added to an existing managed ICT arrangement. - Managed security service for up to 24 months, which includes at least: - active monitoring - human review of alerts - documented incident response arrangements - regular reporting to the customer.	- Renewal of an existing managed security service. - General managed IT support, help desk or system administration. - Response or recovery work relating to an incident that occurred before the application was approved. - One-off assessments, reviews, penetration tests, vulnerability scans or reports. - Cyber security service that does not include active review and management by humans. - Cyber security products supplied without an accompanying managed cyber security service, e.g.: - Automated testing, assessment, monitoring, reporting, risk scoring or compliance platforms where the primary function is software access.	- Maximum funding period is 24 months. - One-off support only. - Quote must separate eligible security services from general ICT services. - Businesses must be able to sustain the service ongoing. - The managed cyber security service must include ongoing monitoring and human review by the provider. Services that rely primarily on automated analysis, automated testing or automated reporting do not meet the requirements of this category.
Software or subscriptions	Security software included in, and necessary for, the approved managed security service (up to 24 months).	- Standalone software subscriptions or licences not related to the managed security service. - Renewal of existing or previously funded software or subscriptions.	Licensing must be itemised or clearly included in the managed service price.
Hardware	N/A	All hardware and equipment.	No hardware is funded under this category.