

Cyber Invest Business Program

Service provider terms and conditions

Acronyms	Full form
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
DCDD	Department of Corporate and Digital Development
DTBAR	Department of Trade, Business and Asian Relations
CIP	Cyber Invest Plan

Contents

1	Purpose	4
2	Objectives.....	4
3	Program overview	4
3.1	Funding amount and rounds.....	4
4	Eligible services	5
4.1	Support categories.....	5
4.1.1	Cybersecurity controls uplift.....	5
4.1.2	Cyber resilience planning.....	7
4.2	Subscription services.....	8
4.3	Excluded services.....	8
5	Service providers	9
5.1	Eligible service providers	9
5.2	In-eligible service providers	10
5.3	Services assessment	10
6	Registration process.....	11
6.1	Before you register	11
6.2	GrantsNT application process	11
6.3	Assessment process.....	12
7	Responsibilities of approved service providers	12
8	Additional responsibilities of listed service providers.....	13
8.1	Additional terms	13
8.2	Suspension from program	14
8.3	Deregistration from program.....	14
9	Funding	14
10	Financial rebates, discounts, financial benefits, and incentives	15
11	Release and indemnity.....	15
12	General terms and conditions	15
12.1	GST.....	15
12.2	Outsourcing and sub-contracting.....	15
12.3	Privacy	16
12.4	Due diligence, audit and compliance with law	16
12.5	Disputes and feedback.....	17
13	Key definitions	17

1 Purpose

These terms and conditions detail the responsibilities and requirements for Cyber Invest Business Program (the program) service providers and are supplementary to the Program Guidelines.

These terms and conditions provide information to assist service providers understand the Cyber Invest Business Program and associated obligations. It outlines the minimum requirements and expectations, providing information on the grants process. This guide should be read in conjunction with the program's terms and conditions for applicants, which may vary at any time.

2 Objectives

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

3 Program overview

The program provides support for Territory small businesses to access professional services from approved eligible service providers to implement a Cyber Invest Plan (CIP) to:

- a) enhance their protection and resilience against cybersecurity threats
- b) reduce the risk of compromise to their business systems and data
- c) avoid business disruption and reputational damage that can result from cyberattacks.

The program will support Territory small businesses to:

- a) invest in cybersecurity controls aligned to international or Australian cybersecurity frameworks, manage cyber controls assurance and enhance related business processes
- b) undertake cyber resilience and preparedness planning or activities.

3.1 Funding amount and rounds

Eligible grant applicants can receive funding of up to \$10,000 to reimburse 50% of the costs of eligible services provided by an approved service provider.

Businesses can access funding across a single or multiple applications within each financial year to a total of \$10,000. Businesses can access funding across a single or multiple applications within each financial year to a total of \$10,000.

Proposed rounds for the programs will be advertised on the [Cyber NT website](https://www.cyber.nt.gov.au/)¹. The number of rounds is dependent on allocated funding and are subject to change without notice.

Once funding allocation is exhausted the program will close until the next funding period.

¹ <https://www.cyber.nt.gov.au/>

4 Eligible services

Eligible service providers will be expected to prepare a CIP proposal as part of quoting under the program.

Professional services available under the program may include:

- a) implementation of cybersecurity controls uplift and associated business policy and process uplift, including implementation of software as a service (SaaS), and cyber assurance
- b) implementation of transition to managed service provider services or cloud services
- c) development/review of business continuity plans to incorporate cybersecurity incidents
- d) development of a cybersecurity incident plan
- e) cybersecurity incident exercise preparedness activities.

The grant applicant must understand their current cybersecurity posture and level of preparedness. to inform the CIP. Service providers will use this information to prepare the plan/s. Undertaking a cybersecurity threat or risk assessment is an excluded service.

Service providers should direct grant applicants to free services facilitated by the Australian Government including the [Small Business Cyber Resilience Service](https://www.idcare.org/smallbusiness)² and [Cyber Wardens](https://cyberwardens.com.au/)³ and guidance published at cyber.gov.au by the [Australian Signals Directorate](https://cyber.gov.au)⁴.

The CIP proposal should not duplicate services available for free to businesses.

The CIP proposal must align with at least one of the following support categories the grant applicant is applying for.

Only one grant will be available for an assurance activity. However, business applicants can apply for multiple grants for cybersecurity controls uplift or another eligible service.

4.1 Support categories

4.1.1 Cybersecurity controls uplift

Prepare a CIP proposal that addresses the following components:

- a) scope of the operating environment (ICT, Internet of Things and Operational Technology) subject to the uplift proposal.
- b) international or Australian cybersecurity standard, framework or guidance being implemented.

Note: Australian Government cybersecurity standards, such as Essential Eight, may be required for contracting to governments and government suppliers.
- c) technical control, business policy, assurance activity or services to be implemented and the related cyberthreats being addressed.

² <https://www.idcare.org/smallbusiness>

³ <https://cyberwardens.com.au/>

⁴ <https://cyber.gov.au>

- d) any SaaS being implemented and the scope of licensing agreements, and implementation services (the grant may contribute to service costs to implement and subscription costs).
- e) any services being transitioned to managed service provider services or cloud services.
- f) confirm a cybersecurity threat or risk assessment has been undertaken to inform a proposal for cybersecurity controls uplift.

A cybersecurity threat or risk assessment is an excluded service for the purpose of the Cyber Invest Business Grant as it should be undertaken prior to the grant application.

Recommended frameworks and/or guidance.

- [Australian Signals Directorate \(ASD\) information security manual \(ISM\)⁵](#)
- [ASD's Essential Eight⁶](#)
- [Strategies to mitigate cyber security incidents⁷](#)
- [ASD's blueprint for secure cloud⁸](#)
- [CIS Controls⁹](#)
- [COBIT¹⁰](#)
- [NIST Cyber Security Framework¹¹](#)
- [ISO27001¹²](#) and [ISO27002¹³](#)
- [Resources for small businesses¹⁴](#)
- [Small business cyber security guide¹⁵](#)
- [Small business cloud security guide¹⁶](#)
- [Ransomware Prevention Guide¹⁷](#)
- [Preparing for and responding to denial-of-service attacks¹⁸](#)

⁵ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism>

⁶ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight>

⁷ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents>

⁸ <https://blueprint.asd.gov.au/>

⁹ [CIS Center for Internet Security](#)

¹⁰ <https://www.isaca.org/resources/cobit>

¹¹ <https://www.nist.gov/cyberframework>

¹² <https://www.iso.org/standard/27001>

¹³ <https://www.iso.org/standard/75652.html>

¹⁴ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security>

¹⁵ <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security/small-business-cyber-security-guide>

¹⁶ <https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/small-business-cybersecurity/small-business-cloud-security-guides>

¹⁷ <https://www.cyber.gov.au/report-and-recover/recover-from/ransomware/protect-yourself-from-ransomware>

¹⁸ <https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/preparing-and-responding-denial-of-service-attacks>

- [Internet of Things devices](#)¹⁹
- [Principles of Operational Technology Cyber security](#)²⁰
- [Protecting industrial control systems](#)²¹
- [Industrial control systems: Remote access protocol](#)²²
- [Secure by Demand priority considerations for Operational Technology Owners and Operators](#)²³
- [Secure your Wi-Fi and router](#)²⁴
- [Domain Name System security for domain owners](#)²⁵

4.1.2 Cyber resilience planning

Develop a CIP proposal to support cyber resilience and/or business continuity for the management of a cybersecurity incident.

Activities may include development of a:

- tailored cybersecurity incident response plan relevant to the grant applicant's operations
- new, or review of an existing, business continuity plan to incorporate cybersecurity incidents and managing the consequences arising from a cybersecurity incident
- a tailored cybersecurity incident exercise and evaluation report,

The CIP proposal must identify if:

- ASD Incident Response Plan templates are to be utilised and tailored
- ASD Exercise in the Box resources are to be utilised and tailored
- the cybersecurity incident type/s subject to the exercise and/or plan.

Recommended frameworks and/or guidance and resources:

- [Ransomware Emergency Response Guide](#)²⁶
- [Email attacks emergency response guide](#)²⁷

¹⁹ <https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-devices/internet-things-devices>

²⁰ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/principles-operational-technology-cyber-security>

²¹ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/protecting-industrial-control-systems>

²² <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/industrial-control-systems-remote-access-protocol>

²³ <https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/secure-by-design/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting-digital-products>

²⁴ <https://www.cyber.gov.au/protect-yourself/staying-secure-online/secure-your-wifi-and-router>

²⁵ <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/network-hardening/domain-name-system-security-domain-owners>

²⁶ https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Ransomware_Emergency_Response_Guide_0.pdf

²⁷ https://www.cyber.gov.au/sites/default/files/2023-04/Email%20attacks_Emergency%20Response%20Guide.pdf

- [Cyber security incident response planning: Executive guidance](#)²⁸
- [Cyber security incident response planning: Practitioner guidance](#)²⁹
- [Exercise in a Box](#)³⁰

4.2 Subscription services

Where the CIP proposal includes subscription to SaaS or managed service providers, the plan must:

- detail the cybersecurity controls provided within the services
- scope of licence subscriptions and duration of the subscription agreement (e.g. annual) proposed to be incorporated within the grant application
- address the cyberthreat and risk areas.

Inclusion of subscriptions to managed services of up to 24 months duration may be accepted subject to a service contract and the grant applicant making payment in full prior to grant acquittal.

Subscriptions to SaaS of up to 24 months duration may be accepted subject to the service provider and grant applicant providing evidence of SaaS licence agreements and subscription payments to the SaaS provider in full prior to grant acquittal.

4.3 Excluded services

The program is unable to support:

- cybersecurity incident response services, including for a current cyberattack incident
- updates to websites that are not related to implementing a cybersecurity control
- services that may be subject to copyright or intellectual property disputes
- services that the eligible provider has not established clear instructions/or advice on the use/ installation, and management of, for the benefit of the eligible recipient
- ongoing cybersecurity audits/assurance activities
- physical security upgrades
- ongoing maintenance with a service provider
- equipment e.g. computers or laptops, or technology already procured, purchased or installed prior to the approval of this grant
- memberships, accreditation, certification, registration or joining fees
- business travel, transport and accommodation costs in relation to the delivery of services
- services from related parties or already being provided through another program or that commenced before funding is approved.

²⁸ <https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cyber-security>

²⁹ <https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cyber-security>

³⁰ <https://www.cyber.gov.au/resources-business-and-government/exercise-in-a-box>

Approved service providers are not permitted to provide funded services under this program where any conflict of interest exists.

5 Service providers

Grant applicants participating in the program can only receive funding for eligible services provided by an approved service provider.

Service providers must submit a Cyber Invest Business Program application form via Grants NT and be assessed and approved as a supplier.

Grant applicants can choose from a list of [approved service providers](#)³¹ on the Business Territory website.

Grant applicants can also nominate any business that meets the 'service provider eligibility' criteria to deliver eligible services.

If the nominated service provider is not an approved provider, the service provider will need to apply for approval and be assessed as successful before the grant application can be assessed. This will result in longer grant application processing times. Listing on the program webpage is optional.

All approved service providers must:

- a) meet the eligibility criteria
- b) pass the service review
- c) agree to and uphold service provider responsibilities
- d) provide 'eligible services' that they have been approved for
- e) adhere to any other relevant terms and conditions as listed in this document and the Cyber Invest Business Program guidelines.

5.1 Eligible service providers

A business is eligible to apply as a service provider if they:

- a) are a Territory Enterprise* (see key definitions); and
- b) are a legal entity (a natural person or an incorporated entity); and
- c) hold a valid Australian Business Number (ABN); and
- d) hold a current Public Liability Insurance and/or Professional Indemnity Insurance policy; and
- e) are able to demonstrate relevant industry certifications and qualifications in ICT and/or cybersecurity and prior business expertise in one or more of the relevant categories under the program for a minimum of 12 months; and

³¹ <https://business.nt.gov.au/help-for-business/applying-for-business-funding-and-grants/service-provider-directory>

- f) hold and maintain during the course of the program all relevant business, occupation and related permits, licences, ICT/cyber industry certifications and insurance coverage required to undertake work in connection with the program, such as public liability insurance or professional indemnity insurance (copies must be provided as evidence on request); and
- g) have an active organisation profile on GrantsNT and successfully register to be part of the program.

Service providers are encouraged to be a member of the [Australian Signals Directorate's Cyber Security Partnership Program](#)³² to receive cybersecurity advice and cybersecurity alerts.

*Exemptions to the Territory Enterprise criteria are available for one off service provisions, when nominated by an eligible applicant and there is evidence that the provision of the service is not available from a Territory Enterprise. Evidence must be provided in the form of a written justification and an 'Industry Capability Network' report. You can submit an enquiry and request on the [ICN NT website](#)³³.

Note: The department will approve or deny the use of a non-Territory Enterprise at its discretion.

Eligible service providers that fail to comply with the program's terms and conditions risk their registration as a service provider being terminated and may face legal action.

5.2 In-eligible service providers

Service providers that will be excluded from the program are those that are:

- a) private or public educational institutions, government agencies and government owned bodies, statutory corporations, and local government bodies
- b) owners/directors:
 - i. that are insolvent or have an undischarged bankruptcy
 - ii. have outstanding grant acquittals or unmet obligations from previous NTG funding.

5.3 Services assessment

Service providers will be required to demonstrate their ability to provide their elected services.

Service providers will need to demonstrate experience or expertise providing services in their nominated areas to small businesses in the last 12 months. When nominating for multiple service areas, two references must be provided for each service area.

All service providers will need to provide:

- a) a business capability statement providing information about the business including services, period of trading in the service area/s, relevant business information and business website
- b) list of employees/subcontractors and their qualifications/certifications and period of experience
- c) two written professional references from previous small business clients related to the service area/s and their contact details.

³² <https://www.cyber.gov.au/partnershipprogram>

³³ <https://icn.org.au/regions/northern-territory/northern-territory-submit-enquiry/>

The below table represents the weighting given to each of the criteria being considered by the assessment panel.

Percentage	Description
30%	Business capability statement outlining services provided, including managed services packages
30%	Evidence of relevant qualifications and length of employment/trading in that field.
40%	Written references demonstrating evidence of works conducted in service areas and outcome. Two references from clients specific to a service area (minimum of 2). If applying for multiple service areas ensure you provide references that cover each area.

Note: The department reserves the right to decide in its discretion if a service provider meets the assessment criteria.

6 Registration process

6.1 Before you register

Read the Cyber Invest Business Program Applicant Terms and Conditions before making an application to register.

Service providers need to be aware of the applicant's rights and obligations in relation to the services being carried out.

6.2 GrantsNT application process

- Login to [GrantsNT](https://grantsnt.nt.gov.au/) ³⁴ under the "Individual profile" linked to the 'Organisation Profile'. If you don't have an "Individual profile" or 'Organisation Profile' you will need to register for these first.
- Complete an online service provider application for the Cyber Invest Business Program and attach all necessary documentation. Applications will not be accepted through other methods such as email, or paper.
- Submit your online application, you will receive an application number via email to the email address registered under the 'Application Contact'.
- Service providers must list and maintain information about employee and subcontractor qualifications/certifications within their Organisational profile.

You will have the option when submitting your application to be listed and promoted as an approved service provider for 24-months. This will require agreement to the additional terms and conditions for listed providers.

³⁴ <https://grantsnt.nt.gov.au/>

6.3 Assessment process

- a) **Application received.** Application received by the department through GrantsNT.
- b) **Applicant and proposal eligibility checked.** Business eligibility conducted by the Departments of Trade, Business and Asian Relations and Corporate and Digital Development. Applications that do not meet eligibility requirements will be returned to the applicant for further information or considered unsuccessful.
- c) **Service review.** An assessment panel (comprised of officials of the Department of Corporate and Digital Development) will review your evidence of expertise in each of your elected service areas. They may request additional proof or information or contact referees if required.
- d) **Recommendations for registration.** The program's assessment panel will make a final recommendation based on their assessment of the application.
- e) **Application outcome.** Applicants will receive a notification of the outcome of their application within an estimated 4 weeks.

Panel assessment – suitability to provide services. An assessment panel of department officials will review the evidence submitted in application and as discovered during the department's due diligence checks.

7 Responsibilities of approved service providers

1. Whilst participating in the program, all approved service providers agree to:
 - a) Provide a quote including a breakdown of costs, expected disbursements and scope of works:
 - i. scope of works should be developed in consultation with the applicant and include agreed milestones and timeline for delivery, reports, deliverables and breakdown of costs including hours.
 - ii. eligible service's expenditure should be separately listed including full details of the proposed service and times within which they will be delivered, and ineligible services should be clearly identified and separate to eligible services.
 - b) Provide a CIP proposal that identifies a cyber threat or risk assessment has been conducted to inform the proposal and states:
 - i. the cybersecurity controls and deliverables or assurance activity to be implemented and refer to the related cybersecurity framework or standards; or
 - ii. the cyber resilience and preparedness planning or activities; and
 - iii. methodology to be used in meeting the objectives and how that will assist the applicant to achieve their objectives, e.g. project plan and client review and acceptance process; and
 - iv. the expected start and completion date and estimated length of time needed to complete the objectives identified (maximum period is 6 months); and
 - v. the individual team members who will work on the project, including how much of the work will be outsourced, or subcontracted (no more than 50%) and their qualifications.
 - c) Act in a professional manner

- d) Provide full disclosure to the grant applicant as to outsourcing or subcontracting to third party providers, elements of work or in entirety, and be contained within the proposal or quotation prior to acceptance of a proposal
- e) Respond in a timely manner to requests from the grant applicant
- f) Be available to complete the work
- g) Deliver services within 6 calendar months of the date of the approved application
- h) Liaise promptly in writing with the grant applicant and the department if no longer able to deliver agreed services within the agreed period
- i) Quote fairly and ensure your quotation represents value for money
- j) Provide the evidence of completed works promptly to the grant recipient after completion of works as part of the grant acquittal requirements.

2. In undertaking the above, service providers must not:

- a) Write or lodge an application for the Cyber Invest Business Program on behalf of a grant applicant
- b) Deliver services that you have not been approved to provide under the program
- c) Make any assumptions about the needs or requirements of the eligible recipient
- d) Act as an agent or a representative of the department in assessing prospective clients' eligibility for the program
- e) Advertise or promote the Cyber Invest Business Program in a way that can be interpreted as you are the only service provider able to provide the service
- i. Or declare or insinuate in any way that they are a preferred service provider of the NTG whether under this program or otherwise.

The following statement is permitted:

"Pre-approved service provider under the NT Cyber Invest Business Program.

For more information about Cyber Invest Business Grant, visit [CyberNT website](https://www.cyber.nt.gov.au/)³⁵.

- f) Provide services to a Cyber Invest Business Program grant applicant or recipient who is a relative or related party of the service provider
- g) Not provide the same services under this program and under another program for the same eligible recipient.

8 Additional responsibilities of listed service providers

8.1 Additional terms

Approved service providers are required to agree to the following additional terms when they opt-in to being listed. Listed service providers agree to:

- a) renew their registration online within six weeks of their 24-month anniversary if they wish to continue as a listed service provider

³⁵<https://www.cyber.nt.gov.au/>

- b) provide the department with written notification if they no longer meet one or more of the eligibility criteria
- c) declare that to the best of the service provider's knowledge, no conflicts of interest currently exist or are likely to arise in their role as an approved service provider
- d) provide written notification to the department and fully disclose all relevant information if a conflict does arise. The service provider must propose and take corrective actions to resolve or otherwise deal with the conflict to the satisfaction of the department
- e) provide written notification of changes to contact details or other published information relating to the service provider
- f) provide written notification of bankruptcy and insolvency.

8.2 Suspension from program

On reasonable grounds the department will suspend a service provider's listing if the department:

- a) receives notice, or otherwise reasonably believes that the service provider no longer meets the eligibility criteria
- b) receives notice, or otherwise reasonably believes that the service provider has an undeclared conflict of interest
- c) is unsatisfied with a service provider's resolution of a declared conflict of interest.

A suspension will remain in effect until the service provider satisfies the department that the service provider again meets the requirements of a listed service provider under these terms and conditions.

8.3 Deregistration from program

A listed service provider will be delisted and have approval status revoked immediately if:

- a) the service provider submits a request to the department
- b) the service provider does not meet the terms and conditions of this program
- c) it is the result of a dispute or complaint resolution process
- d) the service provider contravenes directions agreed to under the program's terms and conditions.

If a service provider is delisted, they will need to re-apply for approval to participate in the program.

Applications from deregistered service providers will be subjected to additional due diligence enquiries.

9 Funding

Funding agreements are between the department and grant applicants. Grant applicants are the business applying for funding through the Cyber Business Program. It is the responsibility of a service provider to invoice and receive payment for services from the grant applicants.

The entirety of funding will be released to grant applicant once the department has received and accepted a copy of evidence of payment for funded works under this program and acquittal of funds. To acquit the grant, recipients are also required to submit evidence of works provided by their service provider, and the final tax invoice. The final invoice must clearly match the quotation provided to the applicant and show amounts received and any amounts outstanding.

This invoice is required by the department to confirm that the financial aspects of the project has been completed in line with the scope approved under the program.

Funding will be provided directly to the grant recipients as a reimbursement, not to the service provider. The department will not remit any invoices on behalf of an applicant participating in the program.

For further details on funding agreements under this program, see the Cyber Business Program Guidelines.

10 Financial rebates, discounts, financial benefits, and incentives

Should any proposed eligible services include services and/or goods/materials that already entitle the eligible recipient to a rebate, discount, or other financial benefit whether from the NTG or not ('benefit'), the grant funding amount or amounts will be reduced by the amount of such benefit to avoid grant duplication.

A eligible service provider must not offer to a grant recipient, and a grant recipient must not ask for or accept from the service provider (or anyone acting on behalf of the service provider), any offer of a benefit (whether monetary or otherwise) to the grant applicant or any third party, as inducement to the grant applicant to accept a quotation, other than the completion of the eligible services set out and described in the quotation. It is okay to reference eligible works and potential Cyber Invest Business Program reimbursable costs.

11 Release and indemnity

By applying to participate and as a continuing obligation throughout any period of participation in the program, the applicant declares and warrants to the department that they have read, understood and fully accept these terms and conditions and fully release and indemnify the department against any loss or damage he/she/it/they may suffer of any nature whatsoever (including without limitation personal injury or death) caused or contributed to by participation in the program.

12 General terms and conditions

12.1 GST

The grant amount is exclusive of any GST.

12.2 Outsourcing and sub-contracting

Full disclosure as to outsourcing or subcontracting to third party providers, elements of work or in entirety, must be declared to the eligible recipient and be contained within the quote. Outsourcing and subcontracting is permitted where:

- a) services are outsourced to another Territory Enterprise*
- b) the department is notified within the quote
- c) no more than 50% of the quoted services are outsourced.

12.3 Privacy

In this section, a reference to “you” is a reference to a participant.

The department is bound by the *Information Act 2002 (NT)* and will only ever use information in accordance with the NTG’s Information Privacy Principles. These principles are available on the [Information Commissioner Northern Territory website](#)²⁸ or call 1800 005 610.

Recipients should read the department’s [Privacy Policy](#)²⁹ and note that by providing information to the department or to any other NT Government agency for the purposes of the program, all participants agree to the following privacy statement:

Information collected as part of the program application process is collected in accordance with the program’s terms and conditions and for the purposes of assessing participant eligibility, audit, monitoring, evaluation, and reporting.

By applying to participate in the program, you consent to the NT Government:

- a) sharing information with any NT Government agencies for the purpose of the department managing and administering services it provides to other agencies
- b) storing information, including personal information (such as names and personal contact details). Personal Information may be stored outside the NT (but not outside Australia)
- c) using the information for the purposes outlined in the terms and conditions of the program and the Privacy Policy and
- d) releasing non-sensitive information, de-identified data in accordance with the NT Government’s open data policy.

If you have provided personal information of another individual to the NT Government, you warrant that you have informed the person to whom the personal information relates that the personal information will be provided to the NT Government, and of the NT Government’s intended use of this personal information, and that you have obtained consent from all such persons to allow the NT Government to use and disclose their personal information in this manner.

12.4 Due diligence, audit and compliance with law

All participants in the program acknowledge:

- a) That the department will conduct such due diligence enquiries as it sees fit in order to ensure the integrity of the program and that the allocated funding is used strictly in accordance with the intent of the relevant government policy. Such enquiries may include (but are not necessarily limited to) company, association and business name searches on a business, title and other searches for the premises, searches of the courts and / or the trustee in bankruptcy and enquiries of private businesses or institutions as the department sees fit; and
- b) That it is a condition of participation in the program that providers and recipients comply with all relevant laws, including the *Payroll Tax Act 2009* and *Taxation Administration Act 2007* and, without limitation, that participants ensure they are aware of their obligations under the *Independent Commissioner Against Corruption Act 2017* (the Act) and that none of their officers, employees, and/or members engage in improper conduct as that term is defined in the Act; and

- c) Participants must exercise utmost integrity and honesty in all their dealings with the department. Misleading and/or deceptive conduct in relation to any aspect of a participant's activity under the program may result in cancellation of the right to participate (including an obligation to repay any monies not already committed).
- d) All participants in the program acknowledge and expressly agree to the department seeking from and sharing information with other NT Government agencies, as well as such external professional advisers as it may need to do in order to assess eligibility, such as conveyancers / solicitors.
- e) Participants must present, upon request by the department within 10 working days of the request, any documentation required by the department that is related to its eligibility to participate in the program and expenditure of any grant made.
- f) The department reserves the right to conduct an audit at any time before or after the completion of the eligible services within 12 months after the program's end date.
- g) By applying to participate in the program, service providers and recipients declare that they expressly agree to the department having access to any private register of information in relation to the provider or recipient, and to the department using, storing, and releasing for lawful purposes, their information, including personal information.
- h) Eligible recipients must provide a statutory declaration in the form and as to the matters as required by the department from time to time and published on the website. Persons who cannot make the declaration truthfully of their own personal knowledge will not have their business admitted participating in the program.

12.5 Disputes and feedback

The department is not responsible for resolving any disputes between recipients and providers. Recipients and providers must conduct their own due diligence regarding their contract to carry out eligible services.

Consumer Affairs can be contacted on 1800 019 319 or go to their website to find information on [dispute resolution](#)³⁶.

The department gives no warranty that these recipients will be able to resolve disputes. If a dispute cannot be resolved in these forums the parties to the dispute will need to take independent legal advice.

For disputes and complaints relating to applications for registration, applications for grant funding and/or funding agreement, the eligible service provider or the eligible recipient can [contact the department](#).³⁷

13 Key definitions

Agreement means a legally binding funding agreement with the Northern Territory Government and a successful grant applicant.

Approved service provider means service providers who have successfully submitted an application to be an approved service provider and been successful.

³⁶ <https://consumeraffairs.nt.gov.au/for-consumers/complaints-and-disputes>

³⁷ <https://dcdd.nt.gov.au/contacts/feedback>

Acquittal is a formal condition of NT Government funding and ensures the obligations of both parties (grant recipient and NT Government) have been met in accordance with the terms of a grant agreement. Acquitting a grant involves a grant recipient providing information which accurately details the outcome of the funded activity, including a report detailing how the monies were spent.

Co-contribution ratio is 50% by the eligible recipient and 50% by the department, unless otherwise specified by the department.

Conflict of Interest means when you have a conflict between your personal and professional duties or associations in relation to this grant.

Cyber Invest Plan proposal means the application for grant funding as submitted by the grant applicant in accordance with the requirements specified in the Grants NT portal.

Department means the Northern Territory Government, Department of Corporate and Digital Development.

Deregistration from program

Deregistration from the program means formally withdrawing a service provider's approval and/or listing in the program.

Deregistered service provider details will be removed from the list service providers.

Eligible recipients will not be able to receive eligible services through deregistered service providers.

Eligible recipient

An eligible recipient is a business that meets the eligibility criteria as listed in the Cyber Invest Business Program Guidelines.

Eligible services

Eligible services are services defined as eligible in the Cyber Invest Business Program Guidelines.

Eligible service provider:

- a) is a Territory Enterprise; and
- b) is a legal entity (a natural person or an incorporated entity); and
- c) holds a valid Australian Business Number (ABN); and
- d) hold a current Public Liability Insurance and/or Professional Indemnity Insurance policy; and
- e) is able to demonstrate relevant prior business expertise in the relevant categories under the program for a minimum of 12 months; and
- f) have an active organisation profile on GrantsNT and successfully register with the department to be part of the program; and
- g) has and will maintain during the course of the program all relevant business, occupation and related permits, licences and insurance coverage required to undertake work in connection with the program.

Evidence of works completed

Evidence of works completed are used to confirm that the service provider has met the grant applicant's business needs as per the quotation and determine value for money. The department may request more information if the supplied evidence is not sufficient.

GST

Goods and Services Tax

NT

Northern Territory

NTG

Northern Territory Government

Professional reference

A professional reference is a written statement from a small business client who you have previously worked with, highlighting the quality of your services, professionalism, and overall satisfaction. Written references must be verifiable by your referee.

Program

The Cyber Invest Business Program.

Registration

Registration is a process of application and assessment. Registration is completed with a successful outcome from an assessment.

Related entity

- a. In the case of a company, a related entity within the meaning of section 50AAA of the *Corporations Act 2001* (Cth), and directors, officers and shareholders of the company and/or a related entity; and
- b. In the case of other incorporated bodies, a member of the board of management of that body or other person that is in a position of influence in respect of decision making of that body; and
- c. In the case of unincorporated bodies, includes sole traders, members of a partnership, joint venturers, and members of the management committee.

Related party

A person, associated or connected (actual, potential or perceived) because of any of the following:

- a. they are a related entity
- b. of a family relationship
- c. of a business partnership
- d. one is a company, and the other is a director or manager of the company
- e. one is a private company, and the other is a shareholder in the company; or

- f. a chain of relationships can be traced between them or their family members under one or more of the above sub-paragraphs.

Relationship (family)

A person connected to you by family (e.g., parents, siblings, aunts, uncles, cousins).

Service provider

A service provider is a company or individual that provides services to this program to others.

Suspension from program

Suspension from the program means temporarily withdrawing your participation or in the program as a service provider.

Suspended service provider details will be hidden from the list of service providers.

Eligible recipients will not be able to receive eligible services from a suspended service provider.

Suspensions will include a list of terms required to be met before the suspension is removed.

Territory Enterprise is a business that satisfies all of the following:

- a) is a legal entity (a natural person or an incorporated entity), with or without a registered business name,
- b) holds a valid Australian Business Number
- c) operating in the Northern Territory - the enterprise is currently engaged in productive activities (i.e. production of goods or delivery of suppliers) within the NT
- d) significant permanent presence - the enterprise maintains an office, manufacturing facilities or other permanent base within the NT,
- e) employs Northern Territory residents

Quote means a written quotation, agreement or contract for the conduct of eligible services between an eligible recipient and an eligible supplier.