

|  |
| --- |
| Rural public health care agencies’ information and communications technology (ICT) Alliance Policy |
| Amended February 2021 |
| OFFICIAL |

|  |  |
| --- | --- |
| To receive this document in another format, email the Digital Health Directorate <digitalhealth@health.vic.gov.au>.  Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.  © State of Victoria, Australia, Department of Health, April 2022. ISBN978-1-76096-786-4 (online/PDF/Word)  Available at Digital Health <https://www2.health.vic.gov.au/hospitals-and-health-services/ rural-health-care-agencies-ict-alliance-policy/digital-health> | |
|  | |

Contents

[1. Introduction 5](#_Toc57987091)

[Amendment 5](#_Toc57987092)

[2. Joint Venture Agreements (JVA) 6](#_Toc57987093)

[3. Governance and management 7](#_Toc57987094)

[3.1 Executive Committee 7](#_Toc57987095)

[3.2 Lead Member 7](#_Toc57987096)

[3.3 ICT Alliance Chief Information Officer 8](#_Toc57987097)

[4. ICT Alliance membership 9](#_Toc57987098)

[4.1 Members 9](#_Toc57987099)

[Mandatory Members 9](#_Toc57987100)

[Non-Mandatory Members 9](#_Toc57987101)

[Membership to more than one ICT Alliance 9](#_Toc57987102)

[4.2 Customers 9](#_Toc57987103)

[5. Guiding principles 10](#_Toc57987104)

[5.1 Provision of Core products and services 10](#_Toc57987105)

[5.2 Provision of non-core ICT products and services 11](#_Toc57987106)

[5.3 Procurement 12](#_Toc57987107)

[Procurement of non-core ICT products and services 12](#_Toc57987108)

[5.4 Probity 12](#_Toc57987109)

[6. Conflicts of interest 13](#_Toc57987110)

[7. Risk management and insurance 13](#_Toc57987111)

[8. Cybersecurity management 14](#_Toc57987112)

[9. Incident management 15](#_Toc57987113)

[10. Financial management 16](#_Toc57987114)

[11. Asset management strategy and planning 16](#_Toc57987115)

[12. Members’ contributions 16](#_Toc57987116)

[13. Reimbursement of costs to Lead Member 17](#_Toc57987117)

[14. Cash payments to the ICT Alliance 18](#_Toc57987118)

[15. Cost efficiency 18](#_Toc57987119)

[16. Reviews of the Rural ICT Alliance Policy 18](#_Toc57987120)

[Attachment 1. List of ICT Alliances and their members 19](#_Toc57987121)

[Attachment 2. Core products and services 24](#_Toc57987122)

# **Introduction**

The *Rural public health care agencies’ information and communications technology (ICT) alliance policy* (the Rural ICT Alliance Policy) outlines the Department of Health (the department) requirements for the operation of information and communication technology by rural health ICT Alliances.

The department expects that ICT Alliances and member health services align their collective and individual ICT Strategies to the Victoria's Digital Health Roadmap for Victoria’s public health sector, using it to develop annual programs, business cases and initiatives for digital health investment across the sector.

The department recognises that common ICT platforms are important for supporting delivery and coordination of public health care and in ensuring the efficient use of government funds.

The department also recognises the ICT Alliances’ achievements and supports their work on facilitating access to core ICT products and services for all publicly funded rural health care agencies.

The Rural ICT Alliance Policy is the primary source document in relation to ICT Alliances.

All ICT Alliance members are required to comply with all applicable law, regulations, orders, rules and government policies, including the Rural ICT Alliance Policy, and to take all steps necessary to monitor and ensure ongoing compliance.

The *Rural ICT Alliance Policy* supersedes *Policy contexts and strategic directions for rural health ICT Alliances* (2 May 2006), the *Rural health Alliances working paper* (May/June 2007) and the *Rural public health care agencies’ alliances policy* Circular number: 17/2008 (June 2008)*.*

## Amendment

This Policy was issued to rural and regional health service in February 2020. Following review of the cost recovery models with health service representatives, the following sections were amended:

|  |  |
| --- | --- |
| Section 3 | Governance and management |
| Section 4 | Alliance membership |
| Section 5 | Guiding principles |
| Section 7 | Risk management and insurance |
| Section 10 | Financial management |
| Section 12 | Member's contribution |
| Section 13 | Reimbursement of costs to Lead Member |

Additionally, the following sections introduced new statements:

|  |  |
| --- | --- |
| Section 2 | Joint Venture Agreement |
| Section 6 | Conflict of interest |
| Section 8 | Cybersecurity management |
| Section 9 | Incident management |
| Section 11 | Asset management strategy and planning |
| Section 12 | Review of the Rural ICT Alliance Policy |

# **Joint Venture Agreements (JVA)**

All public hospitals and public health services established or declared under the *Health Services Act 1988* (the Act), must enter into an Alliance in the region where they are geographically located and operate in accordance with the terms of the joint venture agreement (JVA).

These requirements form part of the funding conditions under the health service agreements entered by the department, or under the relevant statement of priorities, in relation to each of the health services.

The Rural ICT Alliance Policy is the primary source document in relation to the Alliances.

The Rural ICT Alliance Policy must be read in conjunction with the JVA as the JVA sets out in more detail how sections of the Alliance Policy can be executed, effected or realised.

Unless the contrary intention appears, words used in the Rural ICT Alliance Policy have the same meaning as in the JVA.

For avoidance of doubt, the JVA is subject to the Rural ICT Alliance Policy. In the event of any inconsistency, the Rural ICT Alliance Policy prevails.

A review of the Rural ICT Alliance Policy and the JVA will be undertaken periodically. For future changes or revisions to the Rural ICT Alliance Policy, the department may require changes to the JVA to ensure consistency between the two documents.

# **Governance and management**

## 



*Figure 1 – Rural ICT Alliance governance*

## 3.1 Executive Committee

The Executive Committee is the governing body of each ICT Alliance.

The Executive Committee, has the authority to manage the ICT Alliance, including the power to make all approvals, decisions and determinations required or permitted to be given or made by the Members in the ICT Alliance.

The Executive Committee is responsible for leading the development of an annual program and corresponding budget to be recommended for approval by 75 per cent of all ICT Alliance members and, once so approved, for endorsement by the Board.

The Executive Committee is comprised of Chief Executive Officers (CEO) representing ICT Alliance Members. The rules governing Executive Committee membership, terms of reference, their authority and the appointment of an alternate Executive Committee Member are detailed in the JVA.

## 3.2 Lead Member

The lead regional public health service in each of the five regions (or a member regional health service appointed by the Secretary of the department) is required to act as Lead Member for the ICT Alliance.

The Lead Member acts as an authorised agent of the ICT Alliance, the nominated employer of ICT Alliance employees and trustee of the Alliance assets.

The Lead Member is responsible for initiating all actions required to establish the arrangements specified in the Rural ICT Alliance Policy and the JVA which includes convening a special general meeting, in the first instance, for the ICT Alliance to appoint members to the Executive Committee.

As an authorised agent of the ICT Alliance, the Lead Member acts on behalf of members in negotiating, entering into, signing and managing the contracts. It is recommended that any negotiation with vendors or suppliers, including supply contracts to customers, is executed by the Lead Member.

As a trustee of the ICT Alliance assets, the Lead Member will operate a separate bank account for Alliance funds and must ensure that products and services are provided to all Alliance members efficiently and effectively.

The Lead Member, as the nominated employer of the ICT Alliance employees, is responsible for employing Alliance staff, such as Alliance CIO and other staff as deemed necessary and appropriate by the Executive Committee for the purposes of the ICT Alliance, as approved by the members under the Annual Program.

The rules governing Lead Member’s appointment, their powers and duties are detailed in the JVA.

## 3.3 ICT Alliance Chief Information Officer

The Alliance CIO is employed, on behalf of the ICT Alliance, by the Lead Member.

Each ICT Alliance will engage a CIO to manage the Alliance’s business. This includes engagement with Alliance members to establish, implement and monitor service level agreements (SLAs) and key performance indicators (KPIs) as agreed by the Alliance members, to ensure high quality of products and services being delivered by the ICT Alliance.

The duties of the Alliance CIO are set out more fully in the JVA.

# **ICT Alliance membership**

Each ICT Alliance operates as a joint venture.

## 4.1 Members

## Mandatory Members

All registered public health services, public hospitals, integrated community health centres and multi-purpose services within the meaning of the Act, are required to be members of the ICT Alliance in their region. For a list of ICT Alliances and their members, please refer to **Attachment 1**.

All Alliance members are jointly responsible for the operation of the ICT Alliance.

## Non-Mandatory Members

Bush nursing centres, registered community health services and the public sector residential aged care services listed separately for each region, are entitled to become members of the ICT Alliance in their region on the same terms and conditions as the mandatory members. If any of these bodies wish to join the ICT Alliance in the region in which they operate, they will be accepted as members of that ICT Alliance. This will assist these publicly funded health care agencies to receive products and services like those provided to mandatory members, and to be included in the ICT initiatives promoted by the department, where appropriate.

## Membership to more than one ICT Alliance

Dental Health Services Victoria (DHSV) and Ambulance Victoria (AV) may become a member of more than one ICT Alliance, through direct application to those particular Alliances for membership. The Executive Committee of the individual ICT Alliance, upon receipt of the application from DHSV or AV, must consider that application and accept it if in their judgement such membership will not have an impact or adverse effect on the ability of the ICT Alliance to provide core products and services to existing members and will not involve the cross-subsiding of existing members of the prospective member organisation. Please refer to **Section 2 – Governance and management** for more information on the Executive Committee.

## 4.2 Customers

Consistent with the purpose of the Rural ICT Alliance Policy, Alliances can provide products and services to customers (that is, persons or organisations that are not members of the ICT Alliance) on terms set by the Alliance to enhance cooperation and integration between health and community service providers in their region.

These customers may include residential aged care service providers, mental health providers, primary health care networks, private hospitals, day procedure centres, registered funded agencies, general practices, local government bodies and agencies referred to in Section 3.1 as being entitled to non-mandatory membership but elect to be customers of the ICT Alliance in their region instead.

All publicly funded health care agencies, whether customers or non-mandatory members, can only apply for membership in the ICT Alliance in the region in which they operate as the department carefully considers how rural and regional health services are designed, including the local capacity and clinical capabilities, to identify the necessary actions to support safe, high quality and sustainable rural and regional health care service delivery.

# **Guiding principles**

The department recommends that ICT Alliances consider the following key guiding principles:

* **Person-centred health care** – digital health technology investments must deliver integrated solutions that enables person-centred health and well-being for the Victorian health sector. Decision making should place the patient/client at the forefront and is focused on consumer outcomes.
* **Value-based health care** – decisions must be based on the principles that provide value for money, facilitate the realisation of both bankable and non-bankable benefits and assists clinicians in delivering and measuring health care outcomes.
* **Information privacy and security –** given the fast escalating cyber threat landscape, decisions must consider a strategic approach to managing system security, protection of the privacy of patient information and the security and integrity of all information systems.
* **Sustainable health care –** decisions must consider the link between the health and wellbeing of Victorians and the health and wellbeing of the environment and to embed sustainability into the full life cycle of healthcare capital works and health system performance.
* **Robust and transparent governance** – decisions and the decision-making process must be conducted in an open and transparent manner that provide confidence and commitment to all parties.
* **Collaboration -** whilst health services are entitled to realise their own business strategies, all Members must actively engage and collaborate in an ongoing basis to ensure that all needs and perspectives are considered, and equitable and fair solutions are implemented.
* **Change planning** - such as health service mergers, will consider the impact on Alliance cost allocation.

## 5.1 Provision of Core products and services

Each ICT Alliance’s primary purpose is to provide members with the core products and services as listed in **Attachment 2**.

In facilitating the acquisition or supply of ICT products and services from third parties, the Alliance must comply with the policies and protocols established by the Victorian Government Purchasing Board (VGPB) and HealthShare Victoria (HSV) where relevant.

All ICT Alliances and member health services must comply with the service level expectations and security responsibilities as articulated in the department’s *Policy and Funding Guidelines* and JVA *Schedule 2 - Statement of Expectations.*

The following principles apply to the provision of products and services:

* Each ICT Alliance must provide the core products and services to its members equitably, with consideration for the members’ needs.
* Core products and services should be managed and delivered according to standards, interoperability, SLAs and KPIs agreed by members, and where appropriate, relevant state-wide standards.
* The ICT Alliance is responsible for maintaining, replacing and upgrading software and hardware to maintain the provision of core products and services.
* Subject to any transitional arrangements, members are required to acquire or procure core ICT products and services only through the ICT Alliance.
* Members must not enter into any contractual agreements or other arrangements which are in conflict with their obligations under the JVA, or which are otherwise inconsistent with the objectives of the ICT Alliance. This includes on-selling products and services delivered by the ICT Alliance.
* Where the member has an existing contractual agreement/s with a supplier in relation to the supply of a core product or service, the member is expected to terminate such contractual agreement as soon as practicable, and transition to the supply arrangements established by the ICT Alliance. The member must inform the ICT Alliance of any pre-existing contracts and keep the ICT Alliance informed of its plan and timeframe for transitioning to the Alliance arrangements.
* Members must not apply for Federal or State funding for ICT programs or initiatives unless the Member has given the ICT Alliance prior notice of its intention to apply and has received confirmation from the Alliance CIO (on behalf of the ICT Alliance). This is to ensure that any such application aligns with, and does not duplicate nor compete with, an application or proposal made or proposed by the ICT Alliance.
* Grant funding must be sought and used in a manner that is consistent with department policies. It is also recommended that grant funding be used in a manner that demonstrates the receipt of the grant will advance the interests of the ICT Alliance in a strategic and sustainable way.

## 5.2 Provision of non-core ICT products and services

Although the ICT Alliances have a suite of core products and services that must be provided to members, the ICT Alliance may also provide non-core ICT related products and services to members and customers on a case by case basis.

If a member requests that the ICT Alliance provide a non-core product or service, that member may be required to make an additional contribution to the ICT Alliance as determined by the Executive Committee.

The provision of such product or service must be on a full cost recovery basis (commercial basis), ensuring that the price reflects the full cost of service provided (includes capital and recurrent costs), and where relevant, a pro rata share of the existing infrastructure costs and cost adjustments to ensure competitive neutrality with private service providers. The provision of the product or service and must be consistent and in alignment with the department’s policies.

The Victorian Managed Insurance Authority (VMIA) must be notified when any non-core ICT products or services are purchased or provided through the ICT Alliance because of perceived additional risks. Please refer to **Section 5 - Risk management and insurance** for more information.

## Procurement

ICT Alliances are expected to collaborate and consult with HSV for Microsoft Agreement, or any high-value or high-risk ICT hardware procurement activities.

To ensure best value procurement, all ICT hardware procurements must be conducted in a manner consistent with the relevant VGPB, HSV purchasing policies and protocols and the department’s *Policy and Funding Guidelines.* ICT Alliances and member health services are also required to consider recommendations contained the Victorian Auditor-General’s Report [*Procurement Practices in the Health Sector*](https://www.audit.vic.gov.au/report/procurement-practices-health-sector)(October 2011)*.*

The ICT Alliance must convene with the department, through the Chief Digital Health Officer or a delegate to secure the Secretary’s approval, prior to any purchase of ICT products and services over the threshold as required in the *Policy and Funding Guidelines*.

## Procurement of non-core ICT products and services

ICT Alliance members are responsible for their own procurement of non-core ICT products and services. They may wish to do this without the ICT Alliance or through the process set out in Section 4.1.

## 5.4 Probity

All ICT Alliances manage substantial funds.

To ensure public accountability and to conform to legislative and probity requirements, ICT Alliances and member health services are required to consider recommendations contained in the Victorian Ombudsman’s report [*Probity controls in public hospitals for the procurement of non-clinical goods and services*](https://www.ombudsman.vic.gov.au/Publications/Parliamentary-Reports/Probity-controls-in-public-hospitals-for-the-procu) (August 2008) and to ensure strict adherence to processes relating to all transactions. These include:

* a fully documented, transparent and auditable tendering process which includes selection criteria, and no pricing specification in advance
* all pricing arrangements of products and services for members are limited to the agreement collectively acquired by the Alliance on behalf of the members
* negotiation with suppliers is to be undertaken either jointly by members, or by the Lead Member as agent for the members of the ICT Alliance
* should member/s of the ICT Alliance decide to acquire ICT products and services under separate contracts with a common vendor, the price and terms upon which the member/s acquire those products and services must be negotiated through the Lead Member as the agent of the ICT Alliance
* should any ICT Alliance, through the Lead Member, intend to re-supply products and services, the products and services must be paid out of the funds of the ICT Alliance or re-supplied at the originally negotiated price
* any sharing of price information between members about products and services relevant to the activities of the ICT Alliance must be limited to those products and services which are to be the subject of collective acquisition through the ICT Alliance
* any supply contracts to customers must be executed by the Lead Member as agent for the members of the ICT Alliance
* the provision of non-core ICT products and services to members and/or the provision of any products and services to customers are appropriately costed with the charges to reflect the full cost of service provided and competitive neutrality principles
* any refusal to provide ICT products and services should be on the basis of either (a) the provision of those services would not support or enhance cooperation and integration between the health services and community service providers, or (b) the provision of those services do not meet relevant objective and commercial criteria (e.g. concerns about capacity of the customer to pay, any legal risks, or not technically feasible for the ICT Alliance, etc.).

# **Conflicts of interest**

ICT Alliances are required to have written conflict of interest policies and procedures to deal with all conflicts, actual, potential or perceived, covering the Executive Committee, Alliance members, Alliance employees, agents, volunteers and subcontractors.

The Victorian Public Sector Commission has published *Managing conflicts of interest* to assist in the development of conflict of interest policies.

# **Risk management and insurance**

Risk management and assurance activities are essential components of good corporate governance for all organisations, as these activities facilitate better service outcomes and minimise claims and losses. Therefore, management of risk must be an integral part of the ICT Alliance’s culture, reflected in policies, systems and processes.

The *Victorian Government Risk Management Framework* (VGRMF) describes the minimum risk management requirements that agencies are required to meet to demonstrate that they are managing risks effectively. ICT Alliances are expected to have effective and accountable risk management systems and strategies in place which are consistent with the VGRMF and Australian Standard: *AS ISO 31000:2018 Risk Management – Guidelines.*

ICT Alliances are also expected to be cognisant of the Victorian Managed Insurance Authority (VMIA) and its role in supporting agencies in the implementation of the VGRMF.

All ICT Alliances must notify the VMIA of any proposed deviation or departure from the activities specified in the JVA clause 4: *Scope of the agreement* to ensure that the risk is standard or acceptable. For example, it is recommended that ICT Alliances consider buying, rather than building ICT applications, or where possible, consider shared services arrangement for all at-scale ICT services to minimise legal liability risk.

All ICT Alliances must ensure that all members comply with the terms and obligations specified in clause 4: *Scope of the agreement* and clause 17*: Indemnity, liability and insurance* of the JVA and are aware that any activity which may increase the business risk, if not disclosed to the VMIA, may represent a breach of the insurance condition and could result in the VMIA exercising its rights to deny or limit indemnity in the event of a claim.

# **Cybersecurity management**

ICT security is fundamental to the ability of health services to deliver safe and quality patient care through protecting the integrity, confidentiality and availability of clinical and non-clinical data and ICT systems.

In deploying ICT and digital health technology to support service delivery, clinical and non-clinical, all ICT Alliances, member health services and customers, must ensure that local cybersecurity plans, actions and responsibilities comply with:

* *Victorian Government Cyber Security Strategy* including the *Victorian Health Sector Cyber Security Uplift Strategy 72 controls*;
* *Health Sector Cybersecurity Program;*
* National Institute of Standards and Technology (NIST) *Cybersecurity Framework;*
* International Standards for Cybersecurity: ISO 27001/2 and ISO 27018;
* *National eHealth Security and Access Framework* (NESAF) maintained by the Australian Digital Health Agency through its national Cybersecurity Centre; and
* The department’s *Policy and Funding Guidelines.*

The department acknowledges that ICT Alliances have different operating models, capacities and capabilities. However, ICT Alliances and their Regional Public Health Services are expected to work together to provide regional cybersecurity incident reporting, compliance, coordination and monitoring services.

**8.1 Cybersecurity governance –** The ICT Alliance CIOand all member health service Information Technology leaders are required to form a cybersecurity working group that meets on a monthly basis. The purpose of the working group is to ensure collaboration and support on matters of cybersecurity, and continued progress on the *Victorian Health Sector Cyber Security Uplift Strategy 72 controls*.

The ICT Alliance CIO is required to inform the Executive committee on all members’ status on the *Victorian Health Sector Cyber Security Uplift Strategy 72 controls* and report any issues or concerns that may impact the support service delivery, clinical and non-clinical, of the ICT Alliance, member health services and customers.

**8.2 Cybersecurity compliance** – The ICT Alliance CIO is responsible for all Member Health Services who do not have the local capacity and capability to comply with the implementation and ongoing remediation of the 72 baseline controls in accordance with Digital Health’s *Cybersecurity Assurance Framework* and National Institute of Standards and Technology (NIST) *Cybersecurity Framework*.

For Member Health Services with CIOs, the Alliance CIO is expected to provide support, where required, to the respective Health Service CIO, who is responsible for the implementation and ongoing remediation of the 72 baseline controls in their respective health service.

**8.3 Cybersecurity monitoring** – The ICT Alliance is expected to manage and monitor public facing security for data ingress/egress to the internet. The Alliance CIO is responsible for monitoring cybersecurity compliance of all Member Health Services and assist those who do not have the local capacity and capability to monitor their own network environment for threats, suspicious activities and unauthorised programs or program access.

**8.4 Cybersecurity incident reporting**

**8.4.1 Regional Hospital** – ICT incidences that occur at Regional Hospitals must be reported to Digital Health via their respective Health Service CIO. The CIO is also accountable for the coordination of cybersecurity incidents, response and recovery of their respective Health Service. The Alliance CIO’s role is to provide support in the containment and recovery process.

**8.4.2 Member Health Services**

Health Services with CIOs – ICT incidences that occur at Member Health Services, where health services have their own CIOs, must be reported to Digital Health Branch via their respective Health Service CIO. The respective Health Service CIO is also accountable for the coordination of cybersecurity incidents, response and recovery of their respective Health Service. The Alliance CIO’s role is to provide support in the containment and recovery process.

Other member health services - The Alliance CIO is accountable for reporting ICT incidences to Digital Health. The Alliance CIO is also accountable for the coordination of cybersecurity incidents, response and recovery of those Member Health Services.

**8.5 Regional cybersecurity coordination** – The Alliance CIO is responsible for coordinating and supporting the uplift of cybersecurity capabilities of all Member Health Services.

Further information on the role and responsibilities of the ICT Alliance, Alliance CIOs and Member health services are detailed in the JVA *Schedule 2 - Statement of Expectations.*

# **Incident management**

The DHHS Digital Health Branch, in its role as System Manager, needs to be informed of unscheduled critical or major ICT incidents when they occur in health services. In many cases, the Digital Health Branch and the department’s Health Technology Solutions can contribute to resolution of incidents.

Critical incidents are those that impact the delivery of quality and safe care to patients. These are to be reported to the department within one hour of the incident occurring.

Critical incidents also include data breaches and cyber incidents. For more information on cybersecurity, please refer to the Victorian Public Health Sector – Cybersecurity Incident Management Plan.

Major incidents are those that place the delivery of patient safety and care at risk. Incidents that may have a significant clinical impact on business processes are also included in this classification. Major incidents are to be reported within two hours of the incident occurring.

All ICT Alliances and Alliance members must comply with the service level expectations and security responsibilities as articulated in the department’s *Policy and Funding Guidelines* and JVA *Schedule 2 - Statement of Expectations.*

# **Financial management**

The Lead Member will operate a separate bank account for ICT Alliance funds.

Accounting for the activities of the ICT Alliance will be undertaken according to accounting guidelines required under the *Financial Management Act 1994* (Vic), the *Audit Act 1994* (Vic), and the department’s policies and guidelines.

Each Victorian public health service Alliance member is required to disclose, within their financial report, their share of the net result, assets and liabilities of their ICT Alliance. ICT Alliance financial records are subjected to annual audit by the Victorian Auditor General’s Office.

# **Asset management strategy and planning**

Asset management is the coordinated activities, carried out over the asset’s whole lifecycle, to realise the full value from assets in delivering their service delivery objectives. Realisation of value will normally involve a balance of costs, risks, opportunities and performance benefits.

In determining member contributions and service costs for customers, ICT Alliances must exercise due regard to the need to replace all assets at the end of their life cycle and must have an agreed cost-effective replacement strategy in place.

ICT Alliances and member health services should refer to:

* the Victorian Government’s Asset Management Accountability Framework,
* *Asset Management Policy (2018)*,
* the *Strategic Asset Management Plan (2019),* and
* associated guidelines for further information when developing their asset management plans.

# **Members’ contributions**

All members contribute to the funding requirements of the ICT Alliance. In addition to ICT Alliance Principles (refer Section 5), the following principles apply to cost recovery from ICT Alliance Members:

1. The cost recovery methodology is consistent with Department of Treasury and Finance Guidance.
2. Specific areas of focus for future cost models will contemplate equity, full distribution of costs and articulation of the cost recovery method.

Each year, full and transparent information detailing the cost of providing the core ICT products and services is provided to members. This includes ICT Alliance administrative costs, minus costs offset by the provision of non-core ICT products and services to members, and cost offsets from the provision of products and services to customers. This cost will be recovered from members as shown in Table 1, or by applying the current recovery model, for Financial Year 2020/21.

*Table 1 – Rural ICT Alliance cost recovery model 2020/21*

| Proportion of total costs | Cost Recovery. |
| --- | --- |
| 60% | Distributed as a percentage of each Member’s Gross Operating Revenue\* the first $10M |
| 30% | Distributed as a percentage of each member’s GOR\* the next $50M above $10M. |
| 10% | Distributed as a percentage of each member’s GOR\* above $60M. |

\* Gross operating revenue (GOR) figures will be provided by Rural and Regional Health Branch of the department

The GOR calculation is based on the consolidated revenue reported in each agency’s audited financial statements. GOR will be based on *Revenue from transactions* excluding capital grants.

Either the GOR available at the time of calculation, or the GOR for two years prior to the financial year in question can be used in the cost allocation formula (e.g. 2020/21 contributions will be calculated based on 2018/19 GOR because the GOR for the current financial year is not tabled in the Parliament until several months after the end of the financial year).

Each Alliance will review the cost recovery model, and either maintain the approach shown in Table 1, or develop a model supported by its membership for application consistent with DTF guidance, from 1 July 2021.

# **Reimbursement of costs to Lead Member**

ICT Alliance costs are incurred and paid by the Regional Lead Health Service. Each ICT Alliance Member contributes towards these costs under the referred cost recovery model. The budget and cost basis is full cost recovery, including direct, indirect and capital costs. They include costs incurred by the Lead Member for the management of the ICT Alliance affairs, including ICT Alliance staff employment, accommodation, administration and other costs.

ICT Alliance forward planning includes budget preparation and endorsement by the ICT Alliance Executive Committee and Lead Health Service Board. The budget costs will be fully disclosed to the ICT Alliance Executive Committee and recovered from ICT Alliance Members and Customers. Where actual costs or modelled costs are not available, for the purpose of ICT Alliance budget preparation and full cost distribution, overhead allowances are specified in Table 2.

*Table 2 – Calculation of allowances for reimbursement*

| Type of cost | Cost details | Calculation of reimbursement if actual or modelled cost not available |
| --- | --- | --- |
| Administration | Including financial management, audit, human resource management, payroll and procurement | 6% of the total cost of ICT Alliance staff salaries. |
| Accommodation | Appropriate facilities including office space, fuel, light, power, phone and cleaning other utilities. | 4% of the total cost of ICT Alliance staff salaries. |

In the event of a dispute between the Executive Committee and the Lead Member, a request for mediation should be made to the Chief Digital Health Officer in the first instance. The request should be accompanied by cost data, information on competitive pricing and evidence that the costs were incurred within/during the provision of the product and service.

The dispute resolution provisions of clause 18 of the JVA will apply.

# **Cash payments to the ICT Alliance**

Standard member contributions are determined in advance for each financial year following agreement by Alliance members on the year’s program and budget.

Following receipt of advice from the ICT Alliance, the department will facilitate payment of the annual contributions of the members by adjusting the agency cash flow to cover the Alliance contributions either by September of each year or by the sign off of each members’ *Statement of Priorities* (SOPs), whichever is applicable.

# **Cost efficiency**

It is recommended that Executive Committees and Lead Members look for opportunities to contain the costs of core ICT products and services.

The Alliance may provide ICT products and services directly or purchase them from external providers.

In some regions where larger health services have significant parallel infrastructure, rationalisation of ICT Alliance and other infrastructure may represent substantial savings.

# **Reviews of the Rural ICT Alliance Policy**

Each JVA will initially be reviewed 12 months after it commences, then each three to five years after the date of the initial review (Periodic Review). This Rural ICT Alliance Policy will be reviewed by the department between one and two years prior to each Periodic Review of the JVAs.

## Attachment 1. List of ICT Alliances and their members

**Gippsland Health Alliance (GHA)**

| Mandatory members | Non-mandatory members |
| --- | --- |
| * Bairnsdale Regional Health Service (sub-regional health service) * Bass Coast Health * Central Gippsland Health Service (sub-regional health service) * Gippsland Southern Health Service * Kooweerup Regional Health Service * Latrobe Regional Hospital (regional health service) * Omeo District Hospital * Orbost Regional Health * South Gippsland Hospital * West Gippsland Healthcare Group (sub-regional health service) * Yarram and District Health Service | * Buchan Bush Nursing Centre * Cann Valley Bush Nursing Centre * Dargo Bush Nursing Centre * Ensay Community Health Centre Inc. * Gelantipy Bush Nursing Centre * Gippsland Lakes Community Health * Latrobe Community Health Service * Swifts Creek Bush Nursing Centre |

**Grampians Rural Health Alliance (GRHA)**

| Mandatory members | Non-mandatory members |
| --- | --- |
| * Ballarat Health Services (regional health service) * Beaufort and Skipton Health Service * Central Highlands (Hepburn and Kyneton District Health Service) Rural Health * **Djerriwarrh Health Services\*** * East Grampians Health Service * East Wimmera Health Services * Edenhope & District Memorial Hospital * Rural Northwest Health * Stawell Regional Health * West Wimmera Health Service * Wimmera Health Care Group (sub-regional health service) | * Ballarat Community Health * Elmhurst Bush Nursing Centre Inc * Grampians Community Health Centre Inc * Harrow Bush Nursing Centre Inc * Lake Bolac Bush Nursing Centre Inc * Woomelang and District Bush Nursing Centre Inc |

**Hume Rural Health Alliance (HRHA)**

| Mandatory members | Non-mandatory members |
| --- | --- |
| * Albury Wodonga Health (regional health service) * Alexandra District Health * Alpine Health * Beechworth Health Service * Benalla Health * Corryong Health * Gateway Health * Goulburn Valley Health (regional health service) * The Kilmore and District Hospital * Mansfield District Hospital * NCN (Nathalia, Cobram and Numurkah) Health * Northeast Health Wangaratta (sub-regional health service) * Seymour District Memorial Hospital -Seymour Health * Tallangatta Health Service * Yarrawonga District Health Service – Yarrawonga Health * Yea & District Memorial Hospital | * Darlingford Upper Goulburn Nursing Home * Indigo North Health * Nexus Primary Health * Primary Care Connect * Walwa Bush Nursing Centre |

**Loddon Mallee** **Rural Health Alliance (LMRHA)**

| Mandatory members | Non-mandatory members |
| --- | --- |
| * Bendigo Health Care Group (regional health service) * Boort District Health * Castlemaine Health * Cohuna District Hospital * Echuca Regional Health (sub-regional health service) * Heathcote Health * Inglewood & Districts Health Service * Kerang District Health * Kyabram and District Health Service * Maldon Hospital * Maryborough District Health Service * Mildura Base Hospital * Robinvale District Health Services * Rochester & Elmore District Health Service * Swan Hill District Health (sub-regional health service) | * Bendigo Community Health Services Ltd * Northern District Community Health Service Inc. * Mallee Track Health and Community Services * Sunraysia Community Health Services Ltd |

**South West Alliance of Rural Health (SWARH)**

| Mandatory members | Non-mandatory members |
| --- | --- |
| * Barwon Health (regional health service) * Casterton Memorial Hospital * Colac Area Health * Great Ocean Road Health * Hesse Rural Health Service * Heywood Rural Health * Moyne Health Services * Portland District Health * South West Healthcare (sub-regional health service) * Terang and Mortlake Health Service * Timboon & District Health Care Service * Western District Health Service (sub-regional health service) | * Bellarine Community Health Ltd * Balmoral Bush Nursing Centre Inc * Dartmoor & District Bush Nursing Centre Inc |

## Attachment 2. Core products and services

It is the role of the ICT Alliance to provide members with a wide range of core and non-core ICT products and services to meet local priorities and needs.

The minimum set of core products and services that must be provided to members by the ICT Alliance is listed below.

The department strongly recommends for all ICT Alliances to build on the list when planning for their respective core products and services.

1. Connecting to the Clinical Grade Network, including:
2. Using the CGN preferred network vendor
3. Provision of shared services such as connectivity to cloud service providers
4. Internet service, including:
5. Allocated bandwidth for the whole ICT Alliance
6. Access toexternal email and internet browsing
7. Secure remote access to ICT Alliance networks and member services
8. Malware and email filtering
9. Internet edge security solutions to at least restrict:
   * + unauthorised access
     + malware
     + email spam, phishing or similar
     + inappropriate internet content
     + unauthorised data exfiltration
10. Wide area networking (WAN) to support data connectivity between members within the region, the department and administration platforms. This service also includes:
11. WAN management and monitoring, and;
12. Network routing and core switch appliances on all links of shared WAN infrastructure, including agency access routers and uninterruptable power supplies (UPS).
13. Video conferencing (VC) service - including the provision of a central platform to connect VC and telehealth endpoints between members and other health providers.

Note: Management of endpoints are not a part of a core product or service.

1. Core helpdesk services - helpdesk support must be provided for Core services 1-3 above.
2. Voice over Internet Protocol (VOIP) based telephony - includes the provision of a central platform to connect phone calls between members and other health providers.

Note: The provision of telephony handsets and headsets are the responsibility of the respective member

1. Email gateway services including delivery of email outside the network
2. Regional procurement services
3. The Alliance is responsible for the procurement of ICT related core products and services on behalf of Alliance Members.
4. The Alliance may procure ICT related non-core products and services on behalf of Alliance Members as requested.
5. The Alliance and Members are expected to collaborate and consult with HSV for Microsoft Agreement, or any high-value or high-risk ICT hardware procurement activities.
6. The Alliance may procure ICT products for one, many or all Members.
7. Regional advocacy services
8. The Alliance may seek funding for strategic ICT regional initiatives and projects applicable to many or all Members.
9. For core products and services, Alliance Members must not compete with the Alliance for funding.
10. Regional support services for the development of ICT standards, policies, processes and templates for core products and services
11. The Alliance CIO will support members in the development of standards, policies, processes and templates for connectivity, infrastructure, change control and other matters where appropriate.
12. Where Alliance members have their own CIO, the Alliance CIO and the respective health service CIO must collaborate to ensure standards, policies, processes and templates are consistent and applicable to all Alliance Members.
13. Regional representation services
14. The Alliance CIO will represent Alliance Members who do not have a CIO at State ICT forums.
15. Where Alliance members have their own CIO, the respective health service CIO may represent their health service at State ICT forums where appropriate or where Terms of Reference (ToR) allow. The Alliance CIO may represent the health members service from time to time on a case by case basis.
16. Representation services include but is not limited to:
17. Representing members at appropriate forums
18. Advising members about progress, opportunities, issues, options etc.
19. Coordinating activities related to planning and implementation
20. Managing implementations (note: costs for major projects are outside the core products and services)
21. Regional ICT strategic planning services
22. The Alliance CIO is responsible for developing the collective ICT Strategy for all Alliance Members particularly on the provision of core products and services.
23. Where Alliance members have their own CIO, the respective health service CIO is responsible for developing their respective health service ICT strategy, however it must be complementary and compatible with the regional ICT Alliance strategy particularly on the provision of core products and services. There is an ongoing expectation that Alliance CIOs and member health service CIOs work collaboratively to ensure sustainable and system wide benefit to all Alliance Members.
24. Regional cybersecurity services – refer to Section 8 of the ICT Alliance Policy and JVA *Schedule 2 - Statement of Expectations*