CI-ISAC OPERATING RULES

V6.0 (January 2026)

Preamble

Our mission is to build a robust, highly trusted cyber intelligence-sharing *community* and cyber capabilities for Australian Critical Infrastructure owners and operators within and across all sectors to ensure a collective, proactive cyber-resilience posture.

Our values are:

- *Trust*: CI-ISAC is a trusted custodian of members' sensitive information and advisor to support cyber resilience and contribute to collective cyber defences.
- *Integrity*: We take responsibility for safe and secure operations and striving for the highest ethical standards and integrity that underpins our decisions.
- *Agility*: We are able to move, think and adapt quickly as we partner with members to innovate based on their needs and environmental changes to the threat landscape.
- *Excellence*: We exceed best practices in ensuring excellence in the quality of our products, services and interactions.

Therefore, all members agree to follow these rules in their participation in all dealings concerning CI-ISAC (Australia) and their cyber security interactions with other members.

Rules

1. Objectives of CI-ISAC Australia.

1.1. CI-ISAC establishes a critical infrastructure cyber threat intelligence sharing *community* to protect the interests of all Australians through enhanced collective defence of their essential services.

1.2. CI-ISAC brings together the owners, operators, and material suppliers to Australia's critical infrastructure assets, establishing an ecosystem where they can mutually support each other in their own respective cyber security operations by establishing stronger, Australian industry-wide capabilities protecting members' systems of national significance.

1.3. It is not intended to frustrate the wider business interests of any member. Consequently, its mutual cooperation objectives are narrowly confined only to the *cyber security purpose* and matters directly related to that purpose.

1.4. In these rules, *cyber security purpose* means the purpose of protecting an information system of a CI-ISAC Member or a CI-ISAC Participant, and information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

1.5. While information is primarily provided to CI-ISAC, members may voluntarily share information with other members of the community and do so in the best interests of Australian critical infrastructure owners and operators, and of Australians generally.

2. **Definitions**.

2.1. In these Rules and in the activities of CI-ISAC generally, relevant terms are defined in **Schedule 1** below.

3. Parties.

3.1. *Community* means the members, the partners and their employees and agents; the Industry Advisory Group, Academic Research and Development Engagement Group, NCI-TIF and Sectoral TIFs; it includes the CI-ISAC.

3.2. *CI-ISAC* means the governance and operational bodies and activities established and conducted by CI-ISAC Australia Ltd ACN 664 445 907.

3.3. *Community parties* means the corporate entities comprising the members and partners. It does not include CI-SAC Australia Ltd.

4. Principles.

To uphold CI-ISAC values and achieve our mission and objectives, all of our actions are governed by, and the interpretation of these Rules will always be guided by, four Principles.

4.1. *Principle #1: Frankness*.

Within the scope of the cyber security purpose, all members will frankly share their information and intelligence with other members without fear that it will be mis-used by any other member.

4.1.1. Information will only be shared for the cyber security purpose.
4.1.2. Members will take all reasonable action to ensure the information is accurate.
4.1.3. Where information provided is subsequently deemed to be inaccurate, the reporting member must share corrected information as soon as practicable.
4.1.4. Members are not expected to share information that could constitute Member Sensitive Elements of Information (MSEI).
4.1.5. Where other members inadvertently obtain the MSEI of another member, they must promptly destroy the information and discretely notify the affected member without seeking any unfair advantage against any other member or person.
4.1.6. Information submitted to CI-ISAC will be anonymised prior to processing by the NIO to protect the confidentiality of participants.

4.2. *Principle #2: Confidentiality*.

All members will disclose *confidential information* only in accordance with these Rules and definitions stated in **Schedule 3.**

4.2.1. This Principle applies to Priority Intelligence Requirements (PIRs) and Member Information Reporting Needs (MIRNs), as well as any other information that could be relevant to the cyber security purpose of these Rules.
4.2.2. Members will protect the interests of other members by keeping their information confidential.

4.2.3. Specific information sharing conditions are at cl 7.2 below. They do not narrow the broad obligations concerning confidentiality provided for under this Principle.

4.2.4. All information acquired by a member through CI-ISAC is deemed to be confidential information unless the member can reasonably prove otherwise.

4.3. *Principle #3: Cooperation*.

All members will cooperate with other members in the pursuit of the objectives of CI-ISAC.

4.3.1. Members will share relevant information as quickly as operationally practicable.

4.3.2. Members will treat other members with respect in all CI-ISAC dealings, even those outside of the cyber security purpose.

4.3.3. A member may cooperate with any other member to achieve mutually beneficial outcomes within the scope of the cyber security purpose. Cooperating members should share lessons learnt from that cooperation with the NIO for the benefit of the general membership. That sharing must not include any MSEI of any member unless agreement is put in place under cl 7.2.1 below.

4.4. *Principle #4: Non-competition*.

No community party will take any competitive advantage against any other community party arising from anything obtained in their dealings with CI-ISAC.

4.4.1. Noting cl 1.3, 1.4, 4.2.2 and 4.3.3 above and the provisions of these Rules generally, Principle #4 is intended to apply to the cyber security purpose only.

4.4.2. These rules are not intended to enable anti-competitive behaviour as it could be construed under the laws of Australia.

5. **Operating model**.

Key tasks, responsibilities, authorities, accountabilities of elements of the system.

5.1. *CI-ISAC Management Board*.
Strategic direction and priorities are guided by the CI-ISAC Management Board, made up of senior representatives from Australia's Critical Infrastructure sectors. Board members provide thought leadership and guidance to the CI-ISAC executive committee on their respective areas of expertise.

5.2. *CI-ISAC Executive Committee*.
Strategic Execution, Operations and Intelligence are driven by the CI-ISAC Executive Committee made up of senior executives with responsibility for the functional areas that enable CI-ISAC's products and services. The CI-ISAC Executive Committee reports to the Chief Executive Officer and is tasked with delivering the company's strategy.

5.3. *Industry Advisory Group (IAG).*
An Industry Advisory Group guides operational build, effectiveness, and growth made up of representatives at the forefront of cyber defences/intelligence operations for their respective Critical Infrastructure sectors. The CI-ISAC Industry Advisory Group provides an industry-aligned perspective on operational effectiveness, required membership capabilities and potential gaps in the CI-ISAC service catalogue.

5.4. *National Critical Infrastructure Threat Intelligence Forum (NCI-TIF).*

The National CI Threat Intelligence Forum's purpose is to facilitate and enable the sharing of timely, contextual information on threats between members. This information is captured by CI-ISAC's National Intelligence Office (NIO) analysts and used to inform priorities for advisories and intelligence analysis activities. The NCI-TIF is a non-statutory, independent, sectoral, skills-based Group that enables collaboration between CI sector leads. It is not a decision-making body and provides inputs to the collection, analysis, and reporting priorities of the CI-ISAC NIO.

5.5. *Members.*

CI-ISAC serves its members and in turn their customers by building a trusted cyber community and leveraging the best technology in its intelligence platform, resiliency resources, and industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

5.6. *Partners*.

A core aspect of the CI-ISAC ecosystem is our partner network, which through the support of numerous organisations can further the collective resilience of Australia's critical infrastructure entities.

6. **Services**.

6.1. CI-ISAC delivers cyber threat intelligence services through cooperation to build answers to the *Key Membership Questions* (defined in **Schedule 1** and detailed in **Schedule 2)** as information and intelligence is procured with respect to emerging threats, vulnerabilities, recommended countermeasures and mitigations, and other relevant information relating to the cyber security purpose.

6.2. It builds answers to the Key Membership Questions (KMQs) through specific inquiry guided by the Information Requirements.

6.2.1. The Information Requirements provide members with detail on what information to share with the community.

6.2.2. Information Requirements are defined in **Schedule 1** and will be detailed separately.

6.3. By members sharing their information with CI-ISAC and CI-ISAC providing anonymised intelligence with all members within the scope of the cyber security purpose, confidentiality requirements and excluding MSEIs, CI-ISAC contributes to more resilient Australian critical infrastructure.

6.3.1. Members should require their Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) to share event reporting and logs from their member environments in accordance with PIRs, MIRNs and NIO technical specifications.

6.3.2. Members may share CI-ISAC information to TLP WHITE and TLP GREEN classifications with their respective MSPs and MSSPs on the condition it supports the cyber security purpose.

6.3.3. Any information shared under cl 6.3.2 remains the inalienable intellectual property of CI-ISAC and may be shared on the express condition that the sharing member

expressly prohibits the MSP or MSSP from passing the information on to any other person or entity.

6.3.4. Members must not share any information classified TLP AMBER or TLP RED with any MSP, MSSP or any other agent or third party. A contravention of this may be deemed a breach of the membership agreement between the member and CI-ISAC and give rise to membership termination.

6.3.5. Where a member has their MSP/MSSP/third party provider sign a mutual non-disclosure agreement (MNDA) with CI-ISAC, the member can share TLP WHITE, TLP GREEN and TLP AMBER. You, as the CI-ISAC member, are responsible for sharing and forwarding any relevant advisories with your MSP/MSSP/third party provider. Even with a signed MNDA, TLP RED advisories can never be shared with any MSP, MSSP or any other agent or third party.

6.3.6. The members must require MSPs, MSSPs and third-party providers of products or services to adhere to these Rules in the same way that the member itself must.

6.3.7. Nothing in cl 6.3 above prohibits a member from sharing anything with their MSP or MSSP who is also a member of CI-ISAC.

6.3.8. A member and their MSP or MSSP who is also a member may make other arrangements to share MSEI up to TLP AMBER+STRICT under the exception provided in cl 7.2.1.

6.3.9. An MSP or MSSP who is also a member must not share CI-ISAC information to any of its customers who is not a member.

6.4. CI-ISAC Australia Ltd and each partner may make arrangements with each other to provide tailored services to members. The agreement may include:

6.4.1. The partner presents information about the partner's services to members that may be of benefit to members.

6.4.2. The sharing of operational intelligence and information with members via the NIO.

6.4.3. Incentivised service offerings from a partner to members where, if mutually beneficial and in complete transparency of the members and with the agreement of a majority of the IAG, commission may be payable to CI-ISAC for the general benefit of the community.

6.4.4. The NIO provides an assessment of a partner’s service offerings to members, ensuring that assessment is completely independent of the partner’s influence or inducement.

7. **Obligations owed to each other**.

7.1. Members and Partners:

7.1.1. Must take all reasonable steps to ensure any of their agents and employees with access to CI-ISAC systems, intelligence products or any materials carrying a TLP marking other than TLP WHITE are aware of these rules and any associated procedures.

7.1.2. Must at all times conduct themselves in a professional manner in their dealings concerning CI-ISAC information and products, with the public and each other.

7.1.3. Must respect the intellectual property rights of other members.

7.1.4. Must ensure their information systems and user accounts hosting CI-ISAC TLP information comply with technical guidance given under cl 7.3 below.

7.2. When sharing or dealing in shared information, all *participants*:

7.2.1. Must not intentionally share any MSEI outside of their own business or corporate entity for any CI-ISAC purpose without the prior written consent of all parties.

7.2.2. Must immediately notify any other recipient in the event that the participant has inadvertently shared any MSEI with the other recipients, to enable the destruction of the MSEI by the other participants under cl 4.1.5 above.

7.2.3. Must not share any other information (including information satisfying PIRs and MIRNs), intelligence product or other CI-ISAC publication with any other person in contravention of the conditions stipulated in the Traffic Light Protocol (TLP) system.

7.2.4. Must not intentionally deceive any other participant outside of their own business or corporate entity, either to advance their own interests or harm the interests of other participants.

7.2.5. Must correct information previously shared by the participant if the participant subsequently deems that the information was inadvertently incorrect.

7.3. The NIO may provide detailed technical guidance concerning cyber security requirements of participants' IT environments or segments storing or processing CI-ISAC information at various TLP system levels.

7.3.1. The procedure in cl 11.2 below applies to this guideline provision authority.

8. **Communication, media, and public advocacy**.

8.1. The community of CI-ISAC members may authorise the CI-ISAC to advocate publicly on matters of importance to the community.

8.2. Clauses 1.3 and 1.4 limit the scope of matters that the CI-ISAC is authorised to advocate for.

8.3. Authorisation under this clause is granted by majority vote of the members, given on the request of the CI-ISAC via either the NCI-TIF, or broader member vote.

8.4. Authorisation may be specific, limiting advocacy to a particular place, forum or time, or it may be general and enduring, allowing the executive to advocate whenever an appropriate opportunity arises.

9. **Timing of key meetings.**

9.1. The NCI-TIF will meet fortnightly, and may hold additional meetings if required, with the meetings taking place virtually via video conference.

9.2. Member briefing sessions will typically take place the day after the NCI-TIF and will take place virtually via video conference.

10. **Contingency procedures.**

10.1. All members and partners must maintain contingency procedures their entity will execute in the event of a cyber security incident affecting the disclosure of CI-ISAC information from their environments or information systems.

10.2. Those contingency procedures must contain, as a minimum:

10.2.1. In the event a possible incident has been detected, the requirement is that the reporting entity carries out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an incident that has resulted in the disclosure of confidential CI-ISAC information.

10.2.2. The condition that the reporting entity takes all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware of a possible incident.

10.2.3. The condition that the reporting entity submits that report to the NIO within 30 days after the reporting entity becomes aware of the possible incident.

10.2.4. In making the report NIO, the requirement that the reporting entity must specify what CI-ISAC confidential information (defined in **Schedule 1** below) has possibly been exposed, and what TLP markings the entity had assigned to that information.\

10.3. The NIO must analyse the report and notify any other participant if their MSEI information has been inadvertently disclosed.

10.3.1. In making that disclosure, the NIO must ensure that it is kept confidential and take all reasonable steps to obscure the identity of the reporting entity from any other participant.

10.4. Nothing in cl 10.2 above negates the reporting entity's own reporting duties to any other person (either within CI-ISAC or otherwise) to report on any incident arising under law, contract or any other source.

10.5. Upon detecting a possible cyber security incident, the entity must execute the procedures required under this clause.

11. **Amendment of these Rules.**
These Rules may be amended as follows:

11.1. General clauses of these Operating Rules:

11.1.1. By a decision of the Chief Executive Officer (CEO) of CI-ISAC Australia Ltd , subsequently reported to the Board of CI-ISAC Australia and an amended version published to the members..

11.1.2. By a majority vote of the members as facilitated by CI-ISAC leadership at the next Annual General Meeting.

11.2. Detailed technical guidance may be amended by the NIO as required to protect the membership.

11.3. KMQs in **Schedule 2**:

11.3.1. By the decision of the National Intelligence Officer, recorded in writing and distributed to all members for comment and consideration.

11.3.2. Subsequently, by confirmation or veto by majority resolution of the NCI-TIF at its next meeting.

11.4. Information Requirements:

11.4.1. By the decision of the National Intelligence Officer, recorded in writing and distributed to all members for comment and consideration.
11.4.2. Subsequently, by confirmation or veto by majority resolution of the NCI-TIF at its next meeting.

12. **Dispute resolution**. Dispute resolution rules are contained in **Schedule 4** below.

13. **Binding nature of the Rules**

13.1. These Rules are binding on the community parties.

13.1.1. They operate as an extension to the membership or partnership agreement that each party signs on entry into the CI-ISAC community in order to guide all participants' behaviour within that community.
13.1.2. They do not form a contract enforceable by action for contractual damages. This does not affect any other contract made parallel to these Rules associated with membership or partnership agreements or any other contractual agreement.

13.2. **Termination of membership by the Board of CI-ISAC Australia Ltd.** A breach of these Rules constitutes a material breach of the membership or partnership agreement. The Board may terminate the membership of any single member or partner if:

13.2.1. The member or partner has contravened these Rules as determined under Schedule 4.
13.2.2. The arbitration authority executing the dispute resolution under Schedule 4 cl B has recommended that the Board determine whether the impugned entity's membership or partnership be terminated.
13.2.3. Another member or partner has been aggrieved, under reasons determined under Schedule 4
cl B.

13.3. For the purposes of administering and executing these Rules effectively, CI-ISAC Australia Ltd has all the rights of a member of the community.

Schedule 1: CI-ISAC (Australia) Operating Rules definitions

Authorised Activities: means

- Cybersecurity Purpose;
- the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat; or a security vulnerability;
- the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
- the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or
- the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause, or any of the offenses listed in the *Criminal Code Act 1995* (Cth).

CI-ISAC Consumer: means an CI-ISAC participant that receives an Indicator or Defensive Measure through the CI-ISAC Service under these Operating Rules.

CI-ISAC Participant: means a CI-ISAC member or partner that has agreed to share CTI and abide by the CI-ISAC Operating Rules, has accepted these Terms, and paid membership or partnership fees (where applicable).

CI-ISAC Threat Sharing Platform (also "TSP"): means the systems and technologies operated by the CI-ISAC National Critical Infrastructure Threat Intelligence Forum (NCI-TIF), National Intelligence Office, Member Services, and Local/Global cooperation for cyber threat intelligence sharing. The TSP shall not be considered a CI-ISAC Participant, Consumer, or Producer under these Terms.

Confidential information: has the meaning given in the **Schedule 3**. In addition, it also includes any information provided by a member that could be reasonably deemed to include MIRNs, MSEIs or PIRs.

CTI Service: means CI-ISAC's Cyber Threat Intelligence Service, which includes a manual and technical system that enables Cyber Threat Indicator and Defensive Measure sharing between CI-ISAC Members, through the CI-ISAC Threat Sharing Platform (defined below).

CTI Producer: means an CI-ISAC Participant that discloses, through CTI sharing, a Cyber Threat Indicator or Defensive Measure under these Operating Rules.

Cybersecurity Threat: means an action, not protected by law, on or through an information system that may result in an unauthorised effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

Cyber Threat Indicator: means information that is necessary to describe or identify:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat

or security vulnerability;

- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

Key Membership Questions: means enduring, strategic questions that provide the strategic analytical framework around which all CI-ISAC subordinate information requirements are shaped. Specific Key Membership Questions are detailed in **Schedule 2** unless otherwise amended under these Rules.

Information Handling Levels: means, for Indicators and Defensive Measure shared through the Traffic Light Protocol, the requirements for handling, use, and any further sharing that may be permitted in compliance with these Rules. See also **Traffic Light Protocol (TLP) System** below.

Information Requirements: means the MIRNs, MSEIs and PIRs as they are extant from time to time.

Member Information Reporting Needs (MIRNs): means the information that CI-ISAC needs members to report to it to provide tailored cyber threat intelligence to enable Australian critical infrastructure owners and operators to anticipate, mitigate, and respond to cyber threats as part of a peer-to-peer network.

Member Sensitive Element of Information (MSEI): means the elements of information that each member holds that should not be shared with CI-ISAC; examples of MSEIs include legally privileged information, proprietary information, or detailed architectural information.

Participants include:

- all members and partners, and their employees, consultants, authorised third parties, agents and the like, regardless of whether such persons have personally signed any CI-ISAC Mutual Non-Disclosure Agreement as individuals.
- all employees, volunteers, consultants, authorised third parties, or agents engaged by the CI-ISAC Management Board, or Executive Committee (including Operations Divisions and the National Intelligence Office).
- any other person related to a CI-ISAC stakeholder who has access to CI-ISAC or CI-ISAC member information related to the cyber security purpose.
- members' information technology and operational technology Managed Service Providers and Managed Security Service Providers.
- any community party as defined above.

For the sake of clarity MSPs, MSSPs and third-party providers of products or services to members are not community parties. Members are responsible to the extent necessary for MSPs, MSSPs and third party providers whom they introduce into the community.

Priority Intelligence Requirement (PIR): means external threat intelligence requirements defining the intelligence the CI-ISAC needs to incorporate into its threat intelligence products for its members.

Threat Intelligence Forums (TIFs): means the National Critical Infrastructure Threat Intelligence Forum (NCI-TIF) represented by sector champions (leads) to share key threat observations and individual sector-focused TIFs established by the NCI-TIF from time to time.

Traffic Light Protocol (TLP) System: means the Traffic Light Protocol designations, as defined on the CI-ISAC website.

****

Other terms: Other terms have the meaning as defined in the CI-ISAC Lexicon. In the event of an inconsistency between this Schedule and the Lexicon, the meaning in this Schedule takes precedence.

Schedule 2: CI-ISAC (Australia) Key Membership Questions

Key Membership Questions (KMQs) provide the strategic analytical framework around which all subordinate information requirements are shaped. They are worded in the first person from an individual member's perspective to ensure that CI-ISAC delivers the information that is needed by members to help ensure the cyber resilience and continuity of Australia's Critical Infrastructure.

KMQs belong to the members and are maintained by the National Critical Infrastructure Threat Intelligence Forum who act as custodians for the members. Current KMQs are as follows:

KMQ 1. What are the threats that could compromise my operations and cause a local or regional disaster, loss of life or serious personal injury?

KMQ 2. What are the threats that could cause widespread disruption across a critical infrastructure network involving multiple operators, causing regional or national system failure that adversely affects me?

KMQ 3. What are the threats that could lead to me experiencing a reputation-damaging privacy breach?

KMQ 4. What are the threats that could publicly show that I am in breach of Australian or international laws or international standards?

KMQ 5. What are the threats that could lead to a disclosure of my valuable proprietary information or intellectual property?

KMQ 6. What are the threats that could cause me financial loss through permanent loss or temporary denial of critical data (ransomware)?

KMQ 7. What cyber security incidents would prompt me to report a cyber incident to my regulators?

KMQ 8. What indications or threat tactics, techniques and procedures should I monitor or hunt for inside my environments to identify threats to my security posture?

KMQ 9. What risk factors should I monitor for with respect to my upstream supply chain partners?

KMQ 10. What internal event reporting should I prioritise for sharing with other partners and participants in my sector and sub-sector ecosystem?

KMQ 11. What are the critical vulnerabilities in my networks that the threats described above could exploit to cause me loss?

KMQ 12. What countermeasures are other members using to successfully mitigate these vulnerabilities? What countermeasures should I share with others?

Schedule 3: Confidentiality

Confidential Information

Confidential Information means all information of any disclosing party (Discloser) (and its Related Bodies Corporate) that is disclosed to any receiving party (Recipient), for the purposes of sharing threat intelligence information, which by its nature is confidential, is designated as confidential or ought to reasonably be considered to be confidential based on its content or manner of its disclosure, including but not limited to information relating to:

(a) the business, affairs, assets, liabilities, financial position, customers, pricing policies, marketing strategies and business plans of the Discloser and its Related Bodies Corporate;
(b) technology, processes, products, specifications, inventions and designs used or developed by the Discloser and its Related Bodies Corporate;
(c) trade secrets, know-how and information of a commercially sensitive nature, including the existence and terms of this agreement; and
(d) cyber security threats or incidents, but does not include any information to the extent that the:
(e) information was in the Recipient's possession at the time it was first disclosed by the Discloser and was not acquired directly or indirectly from the Discloser;
(f) information is in or enters the public domain, other than through a breach of confidentiality obligations; (f) Recipient receives the information on a non-confidential basis from a person entitled to disclose it; or
(g) information is developed independently by the Recipient without reference, influence, or connection to the Confidential Information.

All Confidential Information is and will remain the property of the Discloser and the Recipient does not acquire any intellectual property rights or other rights to the Discloser's Confidential Information except the limited right to use the Confidential Information for the Purpose in accordance with the cyber threat intelligence sharing purpose. Community parties wish to receive and disclose confidential Information for the purpose of sharing information on cyber threats.

Obligations - Restricted use and disclosure

The Recipient must:

(a) hold Confidential Information in strict confidence and not use or disclose it except as permitted under the Rules or with the prior written consent of the Discloser;
(b) take or cause to be taken all reasonable precautions necessary to maintain secrecy where secrecy is required, and confidentiality and prevent disclosure of Confidential Information (such precautions to include, at a minimum, the precautions the Recipient employs in relation to its own confidential information);
(c) Notify the Discloser promptly if it becomes aware of any unauthorised use or disclosure of the Confidential Information and provide all reasonable assistance to help the Discloser regain possession of the Confidential Information and prevent any further disclosure;
(d) Only use the Confidential Information for the purpose of sharing cyber threat information;
(e) Not reproduce, summarise or modify the Confidential Information except as reasonably necessary to accomplish the purpose of sharing cyber threat information;
(f) Only disclose Confidential Information to an officer, employee, adviser, contractor or agent of the Recipient or of the Recipient's Related Bodies Corporate who has a specific need to have access to

the Confidential Information to accomplish the Purpose and is bound by confidentiality obligations consistent with this agreement; and

(g) ensure that any officer, employee, adviser, contractor or agent of the Recipient or of the Recipient's Related Bodies Corporate to whom the Confidential Information has been disclosed keeps the information confidential and does not use or disclose the Confidential Information other than to the extent permitted by this agreement.

Exclusion

The obligations created in this Schedule do not apply to the extent the Recipient is required to disclose the Confidential Information by:

(a) applicable law, regulation, or legal, regulatory or judicial process or proceeding.
(b) the CI-ISAC Operating Rules
(c) the rules of any stock exchange, or the Australian Taxation Office or any other revenue authority; provided that the Recipient discloses the minimum amount of Confidential Information required to satisfy the law or rules and, before disclosing any information and to the extent permitted by law, the Recipient provides a reasonable amount of notice to the Discloser, and exhausts all reasonable steps to maintain such Confidential Information in confidence, including providing reasonable assistance to the Discloser to obtain a protective order or similar defence against the disclosure request.

Return and destruction.

The Recipient must, on the earlier of expiration or termination of this agreement, immediately cease use of the Confidential Information and if requested to do so by the Discloser, either return to the Discloser, or destroy or delete, as the Discloser directs, all material in hard copy or electronic form that is, contains or utilises Confidential Information, provided that this obligation does not apply to any records required to be retained by law or requirement of a regulatory authority, or to records stored in electronic backups that are reasonably irretrievable.

Survival

The Recipient's obligations of confidentiality and restrictions on use of the confidential Information will survive termination of a participant's agreement with CI-ISAC.

Rights and remedies

In the event of a breach or threatened breach of the Confidentiality requirements, the dispute resolution process outlined in Schedule 4 below will apply. Nothing precludes a member from exercising an applicable legal remedy.

Members and partners agree that they enter into this agreement on their own behalf, on trust for each member of the CI-ISAC community, and on behalf of CI-ISAC and further that any damage or loss suffered or incurred by one participant may be recovered by CI-ISAC, or another member of the CI-ISAC community.

Publicity

No community party may advertise or issue any information, publication, document or article for publication or media release concerning the CI-ISAC community business operations or activities that conflict with CI-ISAC membership or the Rules.

Schedule 4: Dispute resolution

The Principles provided by the Operating Rules cl 4 above require members and other parties to CI-ISAC work as closely as possible to each other within the scope of the cyber security purpose to avoid contravening these Rules. However, if a dispute concerning these Rules arises between community parties, then the dispute must first be resolved through this Schedule.

A. *Mediation*. A member may make a complaint about any other community party alleging a breach of these Rules. The complaint may then be determined by mediation between the parties.

A.1. The complaint must be served on the community party allegedly in breach and on the CEO of CI-ISAC Australia Ltd within six months of the alleged breach.

A.2. The complaint must specify (a) the name of the community party in breach, (b) the name and points of contact of the complaining member, (c) clauses of these Operating Rules allegedly breached, and (d) the particular facts constituting the breach by the breaching community party.

A.3. Within one month of receiving the complaint, the community party allegedly in breach must serve a response to the complaining member and the CEO of CI-ISAC Australia.

A.4. The response must specify (a) whether the member allegedly in breach accepts the complaint and (b) proposes a remedy, or (c) denies the complaint and (d) the factual and interpretive grounds for that denial.

A.5. Within six weeks after receiving the complaint, the CEO of CI-ISAC Australia must appoint a mediator to determine the complaint that all members involved in the complaint agree is acceptable.

A.6. The cost of the mediator will be borne by the complaining member. All other parties must bear all of their own costs themselves.

A.7. The mediator must consider (a) the complaining member's complaint and (b) the response of the community party allegedly in breach and propose a remedy that is fair and equitable considering all of the circumstances.

A.8. The remedy proposal made under cl A.7 above must specify (a) the facts reasonably inferred from the evidence provided by the parties and (b) the breach of the Rules provided by those facts.

A.9. A mediation may be terminated at any time before a final proposal is made by agreement between the parties. The agreement must be served on the CEO of CI-ISAC Australia Ltd as soon as practicable.

A.10. The agreement under cl A.9 above may contain measures that either party agrees to take to resolve the dispute or may provide for no measures whatsoever. Where measures are agreed to, parties who agree to make them must do so under the Operating Rules cl 13.1.

The mediation process is summarised by Figure A below. Figure A does not form a substantive part of these Rules.

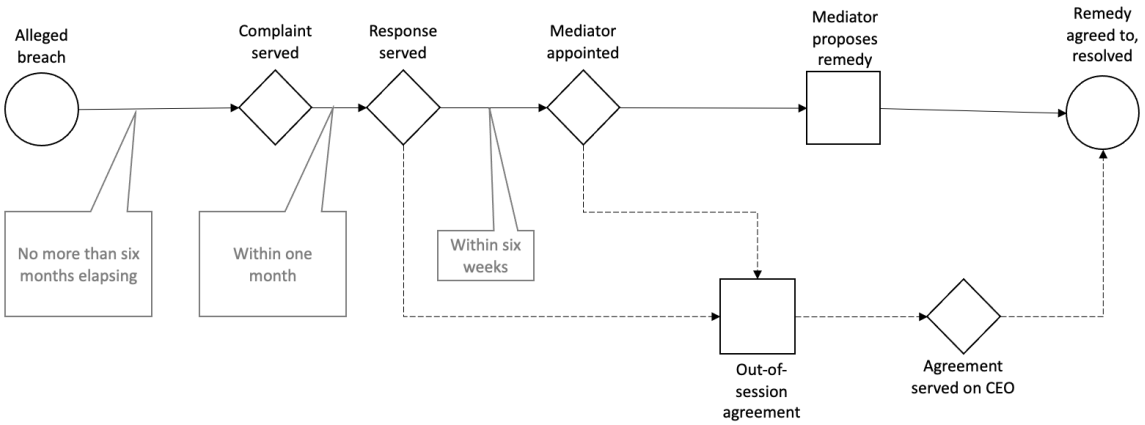

FIGURE A: Dispute resolution, mediation process

B. *Arbitration.* A community party who is the subject of a mediation finding under cl A above may appeal the finding to an independent arbitrator.

B.1. The appeal must be served on the other parties to the mediation and to the CEO of CI-ISAC Australia within 14 days of the final mediation proposal being handed down.

B.2. No community party can file an application for arbitration against another community party unless they are a party to the proposal.

B.3. The appeal must specify (a) the component of the mediator's remedy the appellant appeals, (b) the error in the mediator's interpretation of the Rules and (c) the alternative remedy.

B.4. Any other party who chooses to resist the alternative remedy under cl B.3 being granted must serve a response to the application to all other parties within 14 days after the application is served upon them.

B.5. The response under cl B.4 above must specify the grounds for refusing to grant the alternative remedy.

B.6. The CEO of CI-ISAC Australia must appoint an independent arbitrator within 14 days of receiving the last correctly served response.

B.7. The cost of arbitration will be borne by the appealing party. All other parties must bear all of their own costs themselves.

B.8. The arbitrator may make a finding that (a) a member or other party to the application breached these Rules, (b) require a party to make public statement that they breached these Rules and the remedial steps they will take to prevent similar breaches in the future, (c) find that the community party breach involved aggravating factors, and (d) where aggravating factors exist a recommendation that the party in breach have their membership terminated under cl 13 of the

Operating Rules.

B.9. To avoid doubt, findings under cl B.8 may only mention or bind other parties to the application or CI-ISAC Australia Ltd.

B.10. Orders made by the arbitrator under cl B that require a remedy are binding on all of the parties to the arbitration.

B.11. Orders and reasons made by the arbitrator for any matter must be published and made available for all members within 14 days after the orders are handed down to the parties of the arbitration.

The arbitration process is summarised by Figure B below. Figure B does not form a substantive part of these Rules.

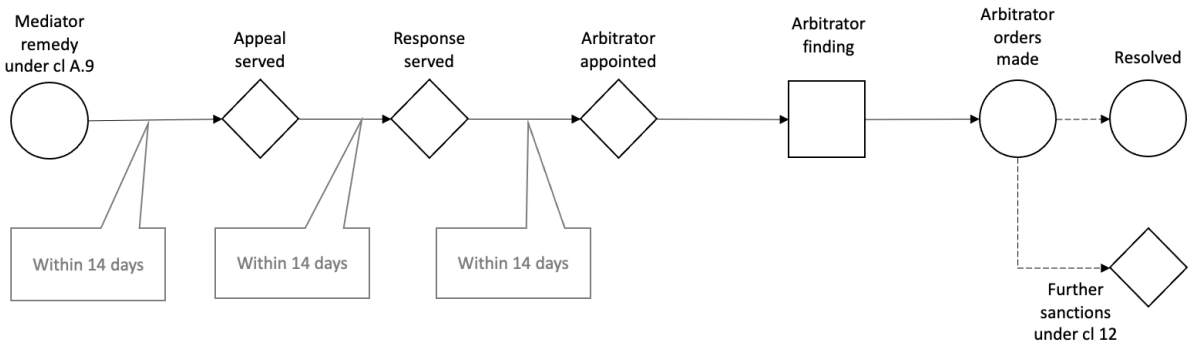

FIGURE B: Dispute resolution, arbitration process

C. Arbitrators' decisions made under cl B create binding precedent for the subsequent interpretation of these Rules.

Last Revised: 23 January 2026

Document history:

Version	Date	Author	Change(s)
6	23/1/26	Patrick Milano	Added clause 6.3.5 to clarify sharing of information with third parties. Added document history table.