INFORMATION SHARING TERMS OF USE

V1.0 (July 2024)

These Terms of Use ("**Terms**") set forth the terms and conditions governing the use of Cyber Threat Indicators and Defensive Measures (defined below) and participation in the Critical Infrastructure Information Sharing and Analysis Centre ("**CI-ISAC**") Australia, Cyber Threat Intelligence Sharing ("**CTI Service**" defined below) community of membership for Cybersecurity Purposes.

1. DEFINITIONS

In these Terms, the following words and terms shall have the following meanings:

1.1. "**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).

1.2. "**CI-ISAC Member**" means a member described in the CI-ISAC Constitution.

1.3. "**CTI Producer**" means an CI-ISAC Participant that discloses through CTI sharing an Indicator or Defensive Measure under these Terms.

1.4. "**CI-ISAC Consumer**" means an CI-ISAC Participant that receives an Indicator or Defensive Measure through the CI-ISAC Service under these Terms.

1.5. "**CI-ISAC Participant**" means a CI-ISAC Member that has agreed to share CTI and abide by the CI-ISAC Operating Rules, has accepted these Terms, and paid membership fees (where applicable).

1.6. "**Authorised Activities**" means:

1.6.1. a Cybersecurity Purpose;

1.6.2. the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat; or a security vulnerability;

1.6.3. 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;

1.6.4. 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

1.6.5. 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).

1.7. "**Cybersecurity 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.

1.8. "**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.

1.9. "**Cyber Threat Indicator**" (hereinafter "Indicator") means information that is necessary to describe or identify:

1.9.1. 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;

1.9.2. a method of defeating a security control or exploitation of a security vulnerability;

1.9.3. a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

1.9.4. 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;

1.9.5. malicious cyber command and control;

1.9.6. the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

1.9.7. any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

1.9.8. any combination of 1.9.1 - 1.9.8.

1.10. "**Defensive Measure**" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability; but does not include a measure that destroys, renders unusable, provides unauthorised access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by (i) the private entity operating the measure; or (ii) another entity that is authorised to provide consent and has provided consent to that private entity for operation of such measure.

1.11. "**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 the CI-ISAC Operating Rules and Traffic Light Protocol (**TLP**).

1.12. "**CI-ISAC Threat Sharing Platforms"** (hereinafter "**TSP**") means the systems and technologies operated by the CI-ISAC National Critical Infrastructure Threat Intelligence Forum, 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.

2. GENERAL RESPONSIBILITIES

2.1. CI-ISAC Members undertake to share Indicators and Defensive Measures broadly for a Cybersecurity Purpose. Each CI-ISAC Participant shall ensure that its use and disclosure of Indicators and Defensive Measures is in accordance with these Terms, applicable law, and any specified Information Handling Levels for Indicators and Defensive Measures. The disclosure of Indicators and Defensive Measures by a CI-ISAC Producer or the TSP shall in no way be construed to imply any kind of license for any intellectual property rights, patents, copyrights, trademarks or trade secrets, without limitation, other than the minimum use necessary for a Cybersecurity Purpose or as otherwise required by law.

2.2. CI-ISAC Participants shall strive to not disclose, advertise, or publicise, without legal compulsion or other legal requirement, the identity of any other CI-ISAC Participant without that CI-ISAC Participant's prior written consent.

2.3. Each CI-ISAC Participant and the TSP to the maximum extent permitted by law, provide no representations or warranties regarding any Indicators or Defensive Measures provided through CI-ISAC Service or CI-ISAC products (advisories, notifications, etc).

2.4. A CI-ISAC Participant may allow others acting on its behalf to support its responsibilities under these Terms, provided those actors have agreed in writing to comply with these Terms.

3. CI-ISAC PRODUCERS

3.1. A CI-ISAC Producer may supply Indicators and Defensive Measures through the CI-ISAC Service for a Cybersecurity Purpose. All submissions of Indicators and Defensive Measures through the CI-ISAC Service by a CI-ISAC Producer will be in accordance with the CI-ISAC Operating Rules. A CI-ISAC Producer may or may not own the Indicator or Defensive Measure or be the source of the Indicator or Defensive Measure it produces.

3.2. An CI-ISAC Producer shall use reasonable efforts to ensure that any Indicator or Defensive Measure shared is accurate at the time that it is supplied. Further, the CI-ISAC Producer will associate any Indicators or Defensive Measures it produces with the appropriate Information Handling Level in compliance with the CI-ISAC Operating Rules, and TLP.

3.3. Each CI-ISAC Producer will use reasonable efforts to remove from any Indicators or Defensive Measures provided to the TSP any information not directly related to a cybersecurity threat that the CI-ISAC Producer knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

3.4. Each CI-ISAC Producer agrees that, in the event that it discloses Indicators or Defensive Measures by mistake, in error, or without their appropriate Information Handling Level (through mismarking or a failure to mark), it shall promptly notify the TSP and take all reasonable steps to mitigate, including sending a versioning update, as soon as it is able.

4. **CI-ISAC CONSUMERS**

4.1. Each CI-ISAC Consumer shall use, handle, and disclose Indicators and Defensive Measures only for a Cybersecurity Purpose and in accordance with their associated Information Handling Level under the TLP.

4.2. Each CI-ISAC Consumer agrees to use reasonable efforts to promptly apply any provided updates representing a change notified by the NIO.

4.3. If requested to do so by the TSP, a CI-ISAC Consumer shall provide a written description of the technical measures and/or protections it has implemented to ensure each Indicator and Defensive Measure is shared only in accordance with its associated Information Handling Level.

5. CI-ISAC TSP RESPONSIBILITIES

5.1. CI-ISAC shall provide notice on its website regarding the process by which an entity may become an CI-ISAC Participant. This process may be updated by the CI-ISAC from time to time, with reasonable prior notice on its website.

CI-ISAC will anonymise the identity of the CI-ISAC Producer of any Indicator or Defensive Measure before sharing the Indicator or Defensive Measure among CI-ISAC Members unless the CI-ISAC Producer consents affirmatively to disclosure of its identity.

6. TERMINATION

6.1. CI-ISAC reserves the right to take any reasonable and lawful action it deems appropriate, including termination of an CI-ISAC Participant's ability to produce or consume Indicators and Defensive Measures for any reason, including the CI-ISAC Participant's response to an TSP inquiry, inadequate response, lack of a response, or continued violation of these Terms.

6.2. All rights and obligations with respect to the disclosure and use of Indicators and Defensive Measures shall survive the termination of these Terms.

Last Updated: 12 July 2024