International Cybersecurity Olympiad 2026 Rulebook

Date: 17/02/2026

Information

Release: Draft

Revisions:

Version	Date	Description
Draft	17 February 2026	Draft Public Release

Changelog

Draft - Draft Public Release

- This should be used solely only as a draft reference, rules may slightly change before the competition date.

1. Introduction

This document is intended to be a comprehensive and self-contained guide for International Cybersecurity Olympiad (ICO) 2026 Contestants. This document is subject to changes depending on feedback and possible organizational updates. Any such changes will be reported in the changelog of this document. If you have any doubts, please reach out to the International Committee or the International Scientific Committee through your country representative.

2. Interpretation

In this document, unless otherwise specified:

1. “Arena” means the physical location in which Contestants will take part in ICO during the competition days.
2. “AI” means Artificial Intelligence.
3. “Contest” or “Competition” or “ICO” means International Cybersecurity Olympiad 2026.
4. “Contestants” or “Competitors” means persons taking part in the competition.
5. “Example” or “e.g.” means a non-exhaustive list of scenarios or things used solely for illustration.
6. “Flag” means a unique, verifiable string associated with a specific task or challenge, which serves as proof of successful completion of a "Subtask", and which must be submitted to the Contest’s platform to receive the points associated with the “Subtask”.
7. “IC” means the ICO International Committee.
8. “ISC” means the ICO Scientific Committee.
9. “Organisers” means the IC, the ISC and the host country.
10. “Subtask” is a part of a task.
11. “Task” means a problem that is presented to the competitors.
12. “TBD” means “To Be Determined”
13. “TBC” means “To be Confirmed”

3. Schedule

The event will be held from June 27th to July 2nd, 2026. Exact schedule TBD.

4. Venue and Logistics

Macquarie University is hosting the event. Macquarie University is located in the northern suburbs of Sydney approximately 15km from the central business district. Macquarie University is reachable by private car and by public transport. The campus is located next to the Sydney Metro and has its own station. More logistical information will be released closer to the event.

5. Staff and Roles

This section gives an overview of the roles involved in the ICO from the contestant point of view. More detailed information is available for team leaders and committee members.

5.1. The International Committee

The IC is a long-term, standing committee, which consists of voting members from different participating countries. The IC is responsible for, among the other tasks, making proposals about future hosts, selecting them, meeting and examining the host organization of the ICO. The IC has a president elected by the participating countries during the ICO from the committee members.

5.2. The Scientific Committee

The ISC is established to work with the Host Country to ensure continuity and quality control for ICO competitions.
The ISC, a long-term standing committee, is responsible for ensuring that problem set has been created, overseeing the test data, and supervising creation and implementation of the grading system. The ISC has a chair elected from and by the committee members. The ISC reports directly to the IC.

5.3. Teams

For the ICO, a Team is a nation, state or a region that has an officially recognized relationship with the United Nations, UNESCO, or which has already taken part in one or more past ICOs.

A National Delegation of a Team is headed by a Delegation Leader.

The status of the Team Delegation can be:

- Participating, the Delegation includes in general a team of one to four Contestants and a Leader and a Deputy Leader, which may not be required;
- Observing, the Delegation may include Leader but no Contestants.

A Contestant is a student who was enrolled at a school for secondary education during the period September to December in the year before the ICO, and is not older than twenty (20) years on the 1st of July of the year of ICO. No polytechnic nor university students are allowed to participate.

6. Competition format, setup and general rules

The event features two separate, 7-hours long, competition days. Each day is completely independent from the other one on the task side (no task is repeated between the two days). On the first day of the event a demo session is planned, where Contestants can test their setup, the internet connection and the game platform.

The competition is planned to be hosted in the cloud. Contestants will reach the competition platform and the tasks through a Wireguard VPN connection.

Each competition day will feature three (3) tasks. Each task is split into subtasks, and it is worth the same fixed amount of points (100). The point value for each subtask is revealed at the beginning of the competition.

At the end of each day a scoreboard is created, where Contestants are ranked based on their total number of points. The final scoreboard is based on the sum of the points gathered by a contestant in the two competition days, in descending order. If more than one Contestants end up with the same number of points, the tie is broken using the sum of the times of their last point increase during each day, in ascending order.

Each task can be seen as a set of jeopardy-style CTF challenges with multiple flags but a common codebase. Each task contains a set of subtasks, granting each a certain amount of points when solved. There is no strict rule about the number of subtasks for each task, expect roughly 4-8 of them. When the correct flag is submitted for a subtask, the corresponding points are awarded. There are no bonus points for being the first one solving a task or subtask, or for particularly clever solutions.

Tasks and subtasks can have different categories in it. Further information is available in the Syllabus section.

7. Allowed software and hardware tools

7.1. Software equipment

Every task proposed during both competition days is guaranteed to be solvable by using just open source or freely available software.

7.2. Hardware equipment

Players are allowed to bring basic hardware equipment setup: **one** laptop each, mouses, keyboards, power, adapters, and external drives. No external monitors or desktop computers are allowed. If something is not mentioned in the list above, it is not allowed, and explicit approval must be sought. This applies to electronics such as bulky objects, which may annoy other teams in the arena. If Contestants are unsure about something, then it is recommended that Contestants request it through their country representatives.

- All Contestants are required to bring all the power adapters they need. Each table will have at least one Type I socket available.
- No additional devices are allowed in the competition arena, including mobile phones. Any such devices found with Contestants will constitute cheating and may result in disqualification.
- Any approved devices brought in should not cause disturbances to other Contestants. In the event of any complaints, watchdogs will decide the merit of the complaint. If the complaint is valid, watchdogs will decide on the appropriate remedy, which may include removal of the device from the Arena. Any decisions made are final and not subject to appeal.

Contestants are required to ensure that the devices they bring are sufficient to solve all tasks in the categories listed in this document. Remote servers are not allowed to be used to augment participants' compute resources. **Since any binary exploitation tasks will be compiled x86_64 binaries, players will need to ensure that they have appropriate tooling on their laptop to solve these tasks.**

Additional equipment must be requested in advance for approval by the organisers. The request must be received via email before (TBD), and its approval/rejection will be communicated to Contestants before (TBD). Contestants must submit all requests via their respective country representatives, unless otherwise specified. All other requests will be ignored. If a request is allowed for a contestant, then it is allowed for all Contestants, unless otherwise specified.

In case of a contestant's hardware failure, Contestants can request to substitute a device. The request must be made through the volunteers in the room, which can either accept it or raise it to the organisers. If the request is accepted, team leaders can bring a new device to the players. The old device will be kept with the organisers and not be allowed to be brought out of the arena.

8. Syllabus and task distribution

8.1. Competition syllabus

Contestants will compete in binary exploitation, cryptography, digital forensics, reverse engineering, web security and miscellaneous tasks. In this section, we provide a brief description of these categories.

- **Binary exploitation.** This category of tasks involves the exploitation of a binary on a remote machine by memory corruption. For the purpose of the competition, binaries will be available only in the x86_64 architecture. Tasks in this category may also include shellcoding and/or escaping constrained environments.
- **Cryptography.** This category of tasks involves understanding and exploitation of modern cryptographic protocols. Vulnerabilities range from heavy mathematical ones to algorithmic/implementation-oriented ones.
- **Digital Forensics.** This category of tasks involves analyzing files with the objective of extracting hidden data from them. Tasks can range from post-exploitation analysis to finding hidden information in images or audio files (steganography).
- **Reverse engineering.** This category requires Contestants to analyze and understand software in the form of compiled binaries, bytecode, obfuscated source code, etc, to extract flags from them.
- **Web security.** This category requires Contestants to analyze custom web applications, possibly exploiting both server and client side vulnerabilities.
- **Miscellaneous.** This category includes tasks that do not strictly fit in the previous ones. Tasks may require skills of mobile security, network security, algorithmic/programming, AI, cloud, radio, etc.

8.2. Task distribution

The rationale behind task distribution is that getting a medal should require skills in a large subset of topics, and being proficient in just one of them is not enough. In general tasks may require skills from different categories and subtasks will involve only a specific one.

The number of points corresponding to each category are similar, as well as the difficulty levels, but **it is not guaranteed** that every category is worth the exact same amount of points. Moreover, it is not guaranteed that the point distribution among categories in the two days of competition remains the same, nor the number of subtasks is (both between problems and between competition days).

Example of a competition day:
Task 1 - 100 points

- Subtask 1 - Cryptography (20 points)
- Subtask 2 - Reverse engineering (15 points)
- Subtask 3 - Binary exploitation (30 points)
- Subtask 4 - Binary exploitation (10 points)
- Subtask 5 - Miscellaneous (25 points)

Task 2 - 100 points

- Subtask 1 - Web security (35 points)
- Subtask 2 - Digital forensics (20 points)
- Subtask 3 - Reverse engineering (20 points)
- Subtask 4 - Cryptography (25 points)

Task 3 - 100 points

- Subtask 1 - Reverse engineering (25 points)
- Subtask 2 - Binary exploitation (10 points)
- Subtask 3 - Miscellaneous (20 points)
- Subtask 4 - Digital forensics (30 points)
- Subtask 5 - Web security (10 points)
- Subtask 6 - Web security (5 points)

8.3. Task examples

TBD

9. Communication and support

9.1. Pre-Event Contact

All Contestants should contact the organisers through their country representatives. Country representatives will be provided with the official point of contact. Email shall be the only medium of contact with the organisers prior to ICO 2026. The organisers will aim to reply to all emails within seven (7) calendar days.

Country representatives and Contestants should ensure that all official communication and information published on the website have been read and any queries have not been addressed prior to contacting organisers.

Any queries related to the information within this document shall be directed exclusively to the ISC.

9.2. Contact during the event

Official Channels

All announcements, clarifications, and updates will be shared exclusively through the official platform and designated channels.

The primary official communication channel is the Discord Server (TBD), which participants will be able to join via the link provided by the organizers (TBD).

Communication rules

Effective communication between Contestants, team leaders and the ICO representatives is essential for the smooth operation of the International Cybersecurity Olympiad. To ensure clarity and efficiency, communication is divided into three categories:

- **Emergencies**, which can cover health and safety issues, but also inappropriate behavior, bullying, discrimination, illegal activities and any situation described in the Code of Conduct for the ICO.
- **Competition-related communication**, which relates to the technical aspects of the competition (e.g. rules, format, technical issues affecting the competition, formal complaints or disputes regarding scoring and rankings, reporting possible disruptive behavior from other Contestants).
- **Event-related communication**, which covers logistics, and any other non-competition matters (e.g., issues with meal schedules and dietary needs, health and safety concerns, general inquiries about event logistics).

For emergencies, feel free to communicate any serious issue in whatever method is most effective and immediate. Examples include:

- Speaking directly with a volunteer inside the Arena or someone from the staff around the venue,
- Open an emergency ticket on the Discord server. (TBD).
- Posting in the dedicated emergency channel on Discord. (TBD).

For competition-related communication, Contestants speak directly with a volunteer inside the arena; volunteers can report urgent or serious issues directly to the relevant committees. Particularly serious situations will be handled case by case.

For all event-related communications, people can always choose between one of the following options:

- The team leader writes a message to the ICO representatives on the Discord channel, explaining what they need.
- A contestant speaks directly with a volunteer inside the Arena; in this case, it will be the volunteer's job to decide whether the request should be handled via the Discord channel or if it needs to be addressed urgently and immediately (e.g. a contestant is not feeling well and needs medical assistance).

Language:

English will be the official language for communication and task descriptions.

10. Use of Artificial Intelligence

Unrestricted AI use is strictly prohibited. All AI use will be monitored through a provided AI chat platform. Any unauthorised use will be investigated and may result in disqualification. Additional details of the capabilities and restrictions put in place will be released at a later time

For the avoidance of doubt, all restrictions listed in section 10 apply exclusively to AI use during the contest. Organizers do not impose any restrictions on AI use during the preparation of the contest.