

# School of Cyber Defense

## Championship rules and consent

Version 2026-08-11 - times are Asia/Dubai

### About the championship

The School of Cyber Defense is a UAE-wide cybersecurity championship for university students, organised by TechFirm Technology LLC, a DESC-certified UAE cybersecurity company. Teams from universities across the Emirates compete through a multi-round format that tests both cybersecurity knowledge and applied defensive skill, and the strongest of them defend their work live at GISEC Global 2026 at the Dubai Exhibition Centre. These rules govern one category: School of Cyber Defense.

### At a glance

Entry is free - there is no fee at any stage. Teams of 1 to 5 students. Registration opened on 12 Aug 2026 and closes on 4 Sept 2026, 15:00 GST. The championship has four stages: registration, online qualification, case & jury, and the live GISEC final on 18 Sept 2026. Travel and accommodation for the final are for participants and their universities to arrange, unless the organiser announces otherwise.

### Eligibility

You must be enrolled as a student at a recognised UAE university or higher-education institution at the time of registration and for the whole championship, studying cybersecurity, computer science, information technology or a closely related programme. Student status is verified manually against the document you upload; unverified applicants and graduates may not compete. Employees of the organiser and of sponsors involved in setting or judging this category, their immediate family, and anyone with access to competition materials that would create an unfair advantage are not eligible.

### Teams

Teams have 1-5 members, one team per participant, and every member must study at the same university. One person creates the team and shares the join code; everyone else registers individually and enters that code. The captain manages the roster, assigns the five qualification blocks among team members, selects the case topic and is responsible for the team upload. Solo entries are allowed but discouraged: the workload is identical whatever the size of the team. Composition locks on 4 Sept 2026; later changes require the organisers.

### What you register with

Your full name in Latin characters exactly as printed on your student document, nationality, a UAE phone number, your university, year of study and major, your academic advisor, and a document proving current student status (PDF, JPG or PNG). Your university email is required and is confirmed with a code before the application is accepted; a personal email is optional. Participants sign in with a one-time code sent to that university address - there is no password to remember. Details must match the proof you provide at verification; inaccurate or incomplete registration may lead to disqualification.

### What the challenge is about

Defensive security engineering for AI systems and government digital infrastructure: threat detection, secure development, and governance, risk and compliance. Your team identifies a concrete risk, builds working software that detects, prevents, verifies or quantifies it, and proves the result with measurements. Every challenge is defensive - none involves attacking systems your team does not own.

## **In scope**

AI and ML security (model extraction, adversarial input, data poisoning, synthetic media detection); applied cryptography (client-side encryption, key management, hash chains, signatures, attestation); infrastructure defense (Zero Trust, micro-segmentation, IoT scanning, denial-of-service mitigation, insider-threat detection on logs); governance, risk and compliance (risk quantification, vendor and supply-chain scoring, identity governance, UAE PDPL obligation mapping, SBOM and CVE analysis); AI infrastructure operations (workload placement, power-aware scheduling, cost and performance modelling, fleet governance, hybrid and air-gapped deployment). Typical tooling: Python or equivalent, Docker, ML and cryptography libraries, simulation and synthetic data, dashboards.

## **Out of scope**

Offensive work against systems your team does not own. Real personal data. Physical hardware and physical security - hardware topics are simulated in software. General application development with no security or AI-infrastructure component. Concept decks without running code. Legal advice.

## **Stages & timing**

Stage 0 - Registration: registration remains open until 4 Sept 2026, 15:00 GST. Stage 1 - Qualification: online qualification runs from 6 Sept 2026, 12:00 GST to 6 Sept 2026, 15:00 GST. Stage 2 - Case & jury: teams that pass qualification select their case topic - places on each topic are limited and go in the order teams take them - and develop and submit their projects from 7 Sept 2026, 12:00 GST to 12 Sept 2026, 11:00 GST. The 6 finalist teams will be announced at 14 Sept 2026, 17:00 GST and will refine their projects with mentor support from 14 Sept 2026 to 17 Sept 2026. Stage 3 - GISEC final: the live final and award ceremony will take place on-site on 18 Sept 2026 at GISEC Global, Dubai Exhibition Centre. Server time (Asia/Dubai) is authoritative. Deadlines are strict and there is no grace period: the platform closes submissions automatically, and a last-minute upload that fails because of a slow connection or an oversized file is not grounds for an exception.

## **Online qualification**

The online qualification consists of five question blocks. The captain assigns all five blocks among the team members, and each block must be assigned to exactly one member. In a five-member team, each member is assigned one block. If a team has fewer than five members, one or more members must complete multiple blocks; a solo participant completes all five blocks. All five blocks must be completed. The team qualification score is calculated across all questions in all five blocks. To progress to Stage 2 - Case & jury, the team must answer at least 70% of all qualification questions correctly.

## **What you submit**

The entry is a presentation that shows the result of all your work on the chosen topic: the problem, what you built or designed, how it works and what it achieves - with evidence such as screenshots, measurements or a recorded walkthrough where you have them. Submit it as a single PDF through the case workspace in your dashboard before the deadline; the size and page limits are shown there, and a short comment for the jury is optional. Feel free to include a short video or a link to your working product in the presentation - it helps the jury see your work in action. Everything - the document, the deck and the live presentation at the final - is in English. Credentials, API keys and personal data are excluded.

## **What we expect of you**

Apply sound cybersecurity principles and current practice rather than dated approaches. Produce original work, with any third-party material properly attributed and licensed. Meet every deadline and follow the submission format exactly. Conduct all activity ethically and lawfully. Be able to explain and defend your work before an

expert panel - justifying your decisions matters as much as the result. Represent your university and the championship professionally, on stage and online.

## **How entries are judged**

Entries pass five sequential review steps: administrative review, technical and compliance assessment, expert judging against the published rubric, finalist announcement, and winner verification. Each entry is scored on five criteria, each scored as a share of its weight: fit to the brief and the business problem (20%), relevance of the proposed solution (15%), whether the prototype works (25%), technical depth and correctness (25%), and innovation (15%) - a 0-100 total. Judges deduct for unsafe methods and unsupported claims. There is no audience vote at any point - attendees may ask questions at the final, but nothing they do affects a score. 6 teams reach the live final. Before a placing is confirmed the organiser verifies originality and eligibility; a team that fails verification loses the placing to the next eligible team.

## **Scoring & appeals**

Multiple-choice is scored automatically; open answers pass automated checks and human moderation. Final standing combines online (50%) and offline (50%) results. A captain may request a score review within 48 hours of publication; a review never changes scores automatically, a human decides. Separately, a team may report a procedural error - an entry left unassessed, a total added up wrongly, a rule applied that is not written here - in writing through the platform within 5 working days of publication, and the organiser answers in writing within 10 working days. A judge's professional assessment of an entry is not open to re-scoring.

## **Prizes and what else you get**

The competition offers a total prize package valued at over AED 20,000, including cash prizes and additional benefits for the winning teams, with certificates of participation for all qualifying teams. Prizes are handed over in person at the award ceremony on 18 Sept 2026 - there is no payout afterwards. At least one member of a winning team must be on stage to receive it; a team absent from the ceremony forfeits its award unless the organiser agreed otherwise in writing beforehand. Beyond the prizes: a stage at one of the region's flagship cybersecurity events, direct contact with sponsors, employers and government stakeholders, public recognition for finalists and winners, and internship opportunities communicated to the captain at the ceremony and confirmed in writing afterwards.

## **How winners are announced**

Winners are announced publicly at the award ceremony during the grand final, and the official results are published afterwards on this platform and the organiser's channels once winner verification is complete. Results are final at that point; the organiser reserves the right to correct any error discovered after the announcement.

## **Fair play**

Answers must be your own. Sharing accounts or work is prohibited. Focus-loss, simultaneous sessions and sign-in anomalies are recorded as reviewable signals; they never disqualify automatically - a human decides.

## **Using AI**

AI tools may assist with development, analysis and drafting, and using them well is encouraged. Two conditions: material AI assistance is disclosed in your documentation, naming the tools and what they did; and the core design and security logic are your own. Fully AI-generated entries are not permitted. At the final any member may be asked to explain any part of the submission, and being unable to do so costs marks. Accuracy, safety and originality remain your responsibility - an error produced by a tool is your error.

## Code of ethics

Act within UAE law and these rules. Never run real attacks, never touch a system your team does not own, never use or expose real personal data - use public or synthetic data only. No plagiarism, no fabricated results, no collusion, no tampering with the platform or scoring. If you find a genuine vulnerability in this platform, report it privately to the organiser instead of exploiting or publishing it. Breaches can mean immediate disqualification and, where warranted, a report to your university or the authorities.

## Your responsibilities

By entering you agree to submit only original work and to attribute third-party components; to use only public or synthetic data and never to test against systems you do not own; to comply with the code of ethics, these rules and UAE law; to provide accurate information and cooperate with verification; to accept the judges' and organiser's decisions as final; to grant the permissions described below; and to behave professionally towards organisers, judges, sponsors, other teams and the public. The organiser may amend the rules, schedule or format where necessary, and will tell registered teams about material changes.

## Your work stays yours

You keep ownership of everything original you create, whether or not you win. By entering you grant the organiser and its named partners a non-exclusive, royalty-free licence to use, reproduce and display the entry - code excerpts, screenshots, the write-up, the deck, the demo, and photography from the final - together with your team name and university, for running, promoting and reporting on the championship. That licence does not permit commercial exploitation, incorporation of your code into a product, or sub-licensing; any of that needs a separate written agreement with you. If part of your submission should stay out of public display, tell the organiser in writing before the final - a reasonable request will be honoured and will not affect judging. You are responsible for making sure your entry infringes nobody's intellectual property or confidentiality: no client-derived or confidential material.

## Personal data (PDPL)

Personal data submitted at registration and during the championship is processed by the organiser under UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, solely to verify eligibility, run the championship, and announce and report results. Verification documents are restricted and audited; advisor details are not used for automated mail. Data is retained for 12 months after the final and then deleted or anonymised, except where a longer period is required by law. It is never sold, and is shared only with the organiser's named partners and service providers to the extent needed to run the event. Export or deletion may be requested from your profile or via [gctf2026@techfirm.ae](mailto:gctf2026@techfirm.ae) (Rania, manager). Withdrawing consent before the final means the entry cannot be assessed and the team leaves the championship; consent is a condition of entry.

## Governing law

These rules are governed by the laws of the United Arab Emirates, and any dispute arising from or connected to the championship falls within the exclusive jurisdiction of the competent UAE courts. Where these rules are published in more than one language, the English version prevails.

## Questions

Is there a fee? No, at any stage. Can we enter more than one topic? No - each team develops one topic. Can I enter alone? Yes, but a full team is strongly recommended. Can I use AI? Yes, within the policy above. What if I miss a deadline? It closes automatically and the work is not assessed. Who owns my work? You do. Who evaluates entries? The judging panel alone, against the published criteria. Anything else: write to Rania, manager, [gctf2026@techfirm.ae](mailto:gctf2026@techfirm.ae). Enquiries are answered Sunday to Thursday, 09:00-17:00 GST, excluding UAE

public holidays; allow up to two working days, and note that questions arriving in the final 48 hours before a deadline may not be answered in time.