Rules of Engagement
2019 Season

Terms

Throughout these rules, the following terms are used:

- White Team - Competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- Black Team - Competition support members that provide technical support and provide overall administrative support to the competition.
- Competition Officials - Representatives of National CPTC charged with the development or execution of the CPTC competition. This will include members of the White Team, Black Team, and other Competition Directors acting in an official capacity.
- Competition / Engagement Team - The institution competitive teams consisting of students competing in a CPTC event.
- Team Captain - A student member of the Red Team identified as the primary liaison between the Red Team and the White Team.
- Team Co-Captain - A student member of the Red Team identified as the secondary or backup liaison between the Red Team and the White Team, should the Team Captain be unavailable (i.e. not in the competition room).
- Team Advisor/Coach - A faculty or staff representative of the Competition Team's host institution responsible for serving as a liaison between competition officials and the team's institution.

Team and Competitor Requirements

Competitor Eligibility

Competitors in CPTC events must be full-time students of the institution they are representing. Team members must qualify as full-time students as defined by the institution they are attending. Competitors may only be a member of one team per CPTC season. Competitors may participate in a maximum of five (5) CPTC seasons. Competitors may not be full time employees of any sponsoring organization. An institution is only allowed to field one team in any CPTC event or season.

Team Composition

Each team must submit a roster of between three and eight (3-8) competitors to the competition director. Rosters will be finalized one week prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CPTC event.

Each competition team may consist of up to six (6) members chosen from the submitted roster. If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition. The remaining two (2) team members will be designated as alternates.

During regional competitions, designated alternates may travel to the regional event and participate in after-hours competition activities, such as report writing and proofreading. These alternates may not interact with team members, the competition environment, or otherwise influence participants or competition officials during competition hours.

Designated alternates will not be permitted to travel to or otherwise assist other team members during the CPTC International Finals.

Changes in Team Composition

Once a CPTC event has begun, a team must complete the competition with the team that started the competition. Substitutions, additions, or removals of team members are prohibited except for extreme circumstances. Team Representatives must petition a member of the White Team in writing for the right to perform a change to the competition team. Working with the competition director, the White Team must approve any substitutions or additions prior to those actions occurring.

Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.

Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.

Institutional Representatives

Each team must have at least one representative present at every CPTC event. The representative must be an active faculty or staff member of the institution the team is representing. Once a CPTC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).

Representatives may not enter their team's competition space during any CPTC event. Representatives must not interfere with any other competing team. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance, deliverables, or presentations with their team during CPTC competition hours and must not attempt to influence their team's performance in any way.

Representatives will be expected to travel with the Competition Team to all CPTC events and participate in activities at the direction of the Competition Officials. Representatives will assist the White Team in scored activities during competition hours at the direction of Competition Officials. Representatives will be expected to fairly and consistently evaluate any scored activities in which they are asked to participate. CPTC officials reserve the right to disqualify any scoring data provided by a representative that is believed to unfairly influence the outcome of the Competition.

Educational Impact

The primary goal of all CPTC events is educational value for the student competitors. Competition Officials will make every effort to accommodate additional learning experiences that do not otherwise

jeopardize the integrity of the competition. If additional educational opportunities are observed during any CPTC event, please share this feedback with the Competition Officials.

Competition Conduct

White Team members may occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow White Team members' access when requested. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by White Team members. Personal input devices, such as keyboards and mice, are permitted provided they do not contain any embedded storage, automation mechanisms, wireless communication hardware, or any other feature that might provide an advantage to a team member beyond ergonomic accommodations.

Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition unless specifically authorized to do so as part of an official competition activity. All hardware related questions and issues should be referred to the White Team. Teams may not remove **any** item from the competition area unless specifically authorized to do so by White Team members including items brought into the team areas at the start of the competition.

Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CPTC events.

Teams must compete without "outside assistance" from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events and development of competition deliverables). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team. Cell phones and other communication devices must be powered off and placed in a designated area within a team's competition room and may not be accessed during the competition hours.

Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.

Team representatives, sponsors, and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.

Teams may only take offensive activity against the target infrastructure in accordance with the Scope of Work (SOW) provided by the Competition Officials. No actions against other competing teams, the Black Team, the White Team, supporting infrastructure, hosting institutions, or publicly available Internet resources will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the White Team, or any global asset will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific targets are considered acceptable, contact the White Team before engaging those targets.

Teams may use any allowed mechanisms to engage the targets, within the confines of the Scope of Work (SOW) and Rules of Engagement (ROE). Any action that interferes with the functionality of the competition environment and supporting infrastructure will result in penalties or ejection against the offending competition team.

All team members will wear badges identifying team affiliation at all times during competition hours. Only White and Black Team members will be allowed in competition areas outside of competition hours.

Internet Usage

Internet resources such as FAQs, how-to's, existing forums and responses, source code, tools, and company websites, are valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee. Only resources that could reasonably be available to all teams before, during, and after the competition are permitted. For example, accessing resources through a corporate sign-in (such as Cisco or VMware) or a private GitHub account are not available and should not be used. The White Team will have final discretion on a case by case basis for material which will be allowed in the competition.

The use of pre-written scripts or code will be permitted under the following circumstances:

- Teams must use a publicly available version-controlled mechanism provided and managed by CPTC for student use for storing any pre-staged scripts or code (eg, a public GitHub repository). The mechanism must clearly identify any changes made to code and the modification dates of any changes. This storage mechanism will be provided by the CPTC Organization for use by competitors.
- Repositories will be identified with the competing institution's name.
- The White Team must be provided a request for access to or the creation of a repository for approval prior to the competition. The submission deadline will be a minimum of two (2) weeks prior to any CPTC event.
- Repositories must be publicly available to anyone, including other CPTC teams and the public Internet at large.
- Teams will be provided access to make changes to their repository.
- All competing teams will be provided, at a minimum, read access to these repositories prior to the CPTC event.
- Teams may be asked to demonstrate or explain their pre-written scripts or code during the event.
- The use of any unauthorized or unapproved repositories will result in penalties or disqualification to the offending team.

Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, email accounts, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. The use of external collaboration and storage environments such as Google Docs/Drive, DropBox, etc. is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas, private email accounts, or storage environments provided for other teams is grounds for disqualification and/or a penalty assigned to the appropriate competition team.

No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.

Internet activity, where allowed, will be monitored and any team member viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through chat/email or any other public or non-public services including sites such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.

All network activity that takes place on the competition network may be logged and subject to public release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

Permitted Materials

No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed on the competition network or machines unless specifically authorized by the White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

Teams may not bring any type of computer, laptop, tablet, PDA, cell phone, smart phone, or wireless device into the competition area unless specifically authorized by the White Team in advance. Cell phones and other communication devices must be powered off and placed in a designated area within a team's competition room and may not be accessed during the competition hours. Any violation of these rules may / can result in disqualification of the team member and/or a penalty assigned to the appropriate team.

Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

Personal input devices, such as keyboards and mice, are permitted for ergonomic purposes provided they do not contain any embedded storage, automation mechanisms, or wireless communication mechanisms.

Professional Conduct

All participants, including competitors, coaches, White Team, Black Team members, and Competition Officials, are expected to behave professionally at all times during all CPTC events including preparation meetings, receptions, mixers, banquets, competition, etc. and within all delivered documents and presentations. In addition to published CPTC rules, host institution policies and rules apply throughout the competition and must be respected by all CPTC participants.

All CPTC events are alcohol free events. No drinking is permitted at any time during competition hours. Activities such as consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated and will result in immediate ejection.

Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by White Team officials. Attempts to circumvent or otherwise violate the spirit of the CPTC rules may be deemed unprofessional conduct at the discretion of the White Team officials or Competition Director.

Competitors behaving in an unprofessional manner may receive a warning from the White Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site.

Competitors expelled for unprofessional conduct will be banned from future CPTC competitions for a period of no less than twenty-four (24) months from the date of their expulsion.

Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director.

Questions, Disputes, and Disclosures

Prior to the Competition

Team captains are encouraged to work with the Competition Director and White Team members to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.

During the Competition

Protests by any team must be presented in writing by the Team Captain to the White Team as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final. All competition results are official and final as of the Closing Ceremony.

In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual or team awards.

In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.

Any vulnerabilities discovered by event participants - especially ones that might be found in vendor equipment - should be considered **private information** and are **not** to be disclosed publicly without the *explicit written* permission of the vendor and coordination with the Competition Director in advance of any publication. Examples of publication venues include but are not limited to: blog posts, white papers, conference proceedings, mailing lists, or other such venues.

Scoring

Scoring will be based on the communication of issues discovered during the assessment, communication during the proposal process, and team actions during the event. Explicit descriptions of how and when the vulnerabilities were discovered and exploited must be provided along with effective and executable mitigation plans for the simulated organization. Issues that might affect ongoing business will need to be addressed as they arise with the simulated organization or White Team officials.

Teams can lose points by violating the Rules of Engagement or Scope of Work agreements or by missing deadlines for deliverables.

Scores will be maintained by the competition officials and may be shared at the end of the competition. By nature, no ongoing scoring will be possible as teams are scored based on deliverables provided to White Team members at various points of the competition.

Any team action that interrupts the competition environment is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, or host institution system, with or without intent, may be disqualified and/or the team assessed penalties. Should any question arise about scoring or how scoring functions, the Team Captain should immediately contact the competition officials to address the issue.

Teams are strongly encouraged to document and address any potential issues they may be causing to a White Team member as soon as possible. Reports addressing such incidents can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, issues or damage potentially caused, etc), a discussion of what was affected, and a remediation plan. A thorough and timely incident report that correctly identifies and addresses such an issue may

reduce the potential penalty for that event – no partial points will be given for incomplete, vague, or untimely incident reports.