|  |  |
| --- | --- |
| Pacific Rim Regional Collegiate  Cyber Defense Competition | March 22 – March 23  2014 |
|  | Team Packet |

**Contents**

[Welcome Letter 2](#_Toc322520660)

[Sponsors 3](#_Toc322520661)

[Map & Directions 4](#_Toc322520662)

[Schedule 5](#_Toc322520663)

[Competition Overview 6](#_Toc322520664)

[Mission 6](#_Toc322520665)

[Event Objectives 6](#_Toc322520666)

[Terminology 6](#_Toc322520667)

[PRCCDC Regional Competition Rules 7](#_Toc322520668)

[Prohibited Items 7](#_Toc322520669)

[Professionalism 7](#_Toc322520670)

[Scoring Overview 7](#_Toc322520671)

[Availability Scoring 8](#_Toc322520672)

[Inject Scoring 8](#_Toc322520673)

[Inject Time Management 9](#_Toc322520674)

[Attack Scoring 9](#_Toc322520675)

[Incident Reporting 9](#_Toc322520676)

[CCDC National Competition Rules 10](#_Toc322520677)

[Competitor Eligibility 10](#_Toc322520678)

[Team Composition 10](#_Toc322520679)

[Team Representatives 11](#_Toc322520680)

[Competition Conduct 11](#_Toc322520681)

[Internet Usage 12](#_Toc322520682)

[Permitted Materials 13](#_Toc322520683)

[Professional Conduct 13](#_Toc322520684)

[Questions, Disputes, and Disclosures 14](#_Toc322520685)

[Scoring 14](#_Toc322520686)

# Welcome Letter



Highline Community College logo link to home page

**To the Participants of the Pacific Rim Regional Collegiate Cyber Defense Competition:**

As the Chair of the Pure and Applied Science Division of Highline Community College and Regional Director of the Pacific Rim Regional Collegiate Cyber Defense Competition (PRCCDC), I would like to welcome you to the 7th Annual Cyber Defense Competition. This year we have 13 teams competing along with students from at least one high school getting the lay of the land.

|  |  |
| --- | --- |
| * DeVry University | * Linfield College |
| * Evergreen State College | * University of Idaho |
| * Green River Community College | * University of Washington - Bothell |
| * Highline Community College | * University of Washington - Seattle |
| * ITT Tech - Boise | * University of Washington - Tacoma |
| * Lewis & Clark College | * Western Washington University * Whatcom Community College |

We expect this to be a profound learning experience for students and an opportunity to incorporate network security concepts from the contest into the curriculum at your respective schools. The web site at [www.prccdc.corg](http://www.prccdc.corg) has some information you need to prepare for success in this event.

If you have further questions, please feel free to contact me either by email or phone at the numbers below.

Kind regards,

Dr. Amelia Phillips   
Chair, Pure and Applied Science Division

CIS and Computer Science Departments

Regional Director PRCCDC

aphillips@highline.edu  
206-592-3497

# Sponsors

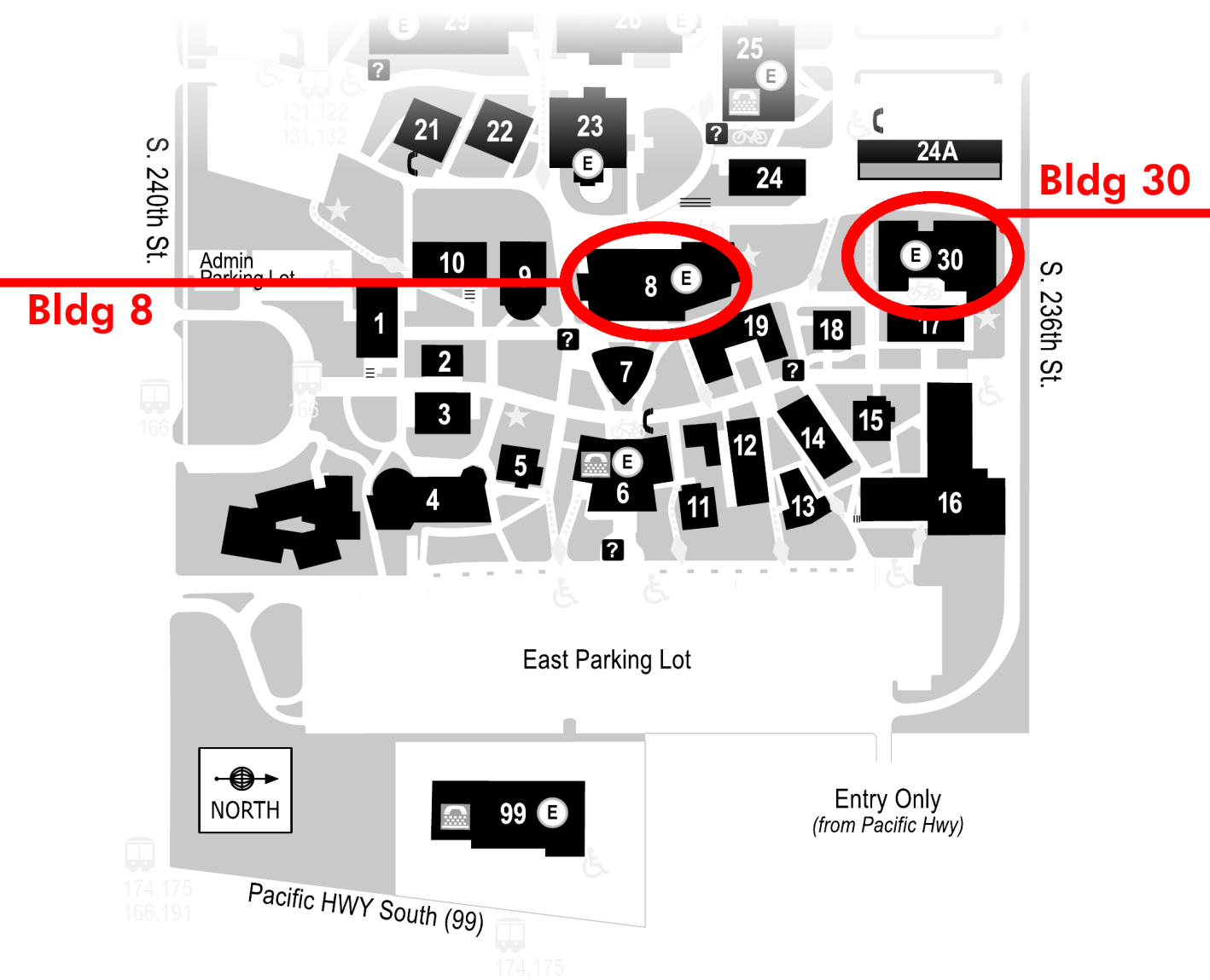
It is through generous donations of time, equipment, knowledge, and funds that this event is made possible.  
In addition to the numerous volunteers, the PRCCDC wishes to thank the following sponsors:

Highline Community College logo link to home page

# Map & Directions

The venue for the competition is Highline Community College. Free visitor parking is available on the days of the competition in the East Parking Lot (no permit required). PRCCDC events are held in Building 8 and Building 30. Breakfast and dinner are served in Building 8.

|  |  |
| --- | --- |
| **Highline Community College** 2400 S. 240th Street Des Moines, WA 98198 | From Seattle: Take Interstate 5, exit 149 From Tacoma: Take Interstate 5, exit 149B   * Proceed west on Kent-Des Moines Road to Pacific Highway South * Turn left (south) onto Pacific Highway South * Turn right (west) onto South 240th Street * Entrance to the East Parking Lot is on the right |



# Schedule

|  |  |
| --- | --- |
| Saturday, March 22, 2012 – Competition Day 1 | |
| 8:00 AM – 9:00 AM | **Registration & Breakfast**  Location: Bldg 8 (Mt. Townsend) |
| 8:15 AM – 8:30 AM | **Opening Announcements**  Location: Bldg 8 – *Led by Amelia Phillips* |
| 8:30 AM – 9:00 AM | **Team Packet Review**  Location: Bldg 8 – *Led by Idaho State University White Team* |
| 9:00 AM – 7:00 PM | **Competition Session Day 1**  Students will compete through lunch. Boxed lunches provided. Snacks provided outside of competition rooms |
| 11:30 AM – 1:00 PM | **Boxed Lunches**  Location: Bldg 30 – in competition rooms |
| 7:00 PM – 9:00 PM | **Networking Dinner – Students meet with Sponsors**  Location: Bldg 8 (Mt. Constance/Mt. Olympus) |
| 9:00 PM | **End of Competition Day 1** |

|  |  |
| --- | --- |
| Sunday, March 23, 2012 – Competition Day 2 | |
| 7:15 AM – 8:00 AM | **Hearty Breakfast**  Location: Bldg 8 (Mt. Constance/Mt. Olympus) |
| 8:00 AM – 4:30 PM | **Competition Session Day 2**  Location: Bldg 30 |
| 11:30 AM – 1:00 PM | **Boxed Lunches**  Location: Bldg 30 – in competition rooms |
| 4:30 PM | **Competition Ends**  Location: Bldg 30 |
| 4:30 PM – 5:30 PM | **Dinner**  Location: Bldg 8 (Mt. Constance/Mt. Olympus Room) |
| 5:30 PM – 6:30 PM | **Debrief by White Team and Red Team**  Acknowledgements and Winner Announced |
| 6:30 PM | **End of Competition Day 2** |

# 

# Competition Overview

PRCCDC is a two-day event focusing on the operational aspect of managing and protecting an existing commercial network. It provides a unique opportunity for students and industry professionals to interact and discuss many of the security and operational challenges the students will face as they enter the job market.

You have just been hired as the network and security administrators at a small company and will be taking administrative control of all information systems. You know very little about the network, what security level has been maintained, or what software has been installed. You have limited time to familiarize yourself with the network and systems and to begin security updates before the Red Team starts attacking your company. In the midst of all the commotion, you have to keep up with the needs of the business and maintain availability of critical Internet services.

## Mission

The Collegiate Cyber Defense Competition system provides institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting business information systems and a corporate network infrastructure.

## Event Objectives

* Build a meaningful mechanism by which institutions of higher education may evaluate their programs.
* Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work.
* Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams.
* Create interest and awareness of the information assurance profession among participating institutions and students.

## Terminology

* **Gold Team:** The organizing team that oversees the event and has final say on all disputes
* **White Team:** The competition officials that evaluate team performance and enforce rule compliance.
* **Red Team:** The penetration testing professionals simulating external hackers attempting to gain unauthorized access.
* **Black Team:** The competition support members that provide technical and administrative support.
* **Blue Team/Competition Team:** The student teams competing in the CCDC event.
* **Orange Team:** Customers who call with complaints or issues such as password changes
* **Team Captain:** A student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team.
* **Team Co-Captain:** A student member of the Blue Team identified as the backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable.
* **Team Representatives:** A faculty or staff representative of the Blue Team’s host institution.

# PRCCDC Regional Competition Rules

## Prohibited Items

The following items are not allowed in the competition rooms. **There will be a central area outside of the competition rooms where these items can be safely stored.**

* Backpacks, fanny packs, purses
* Cell phones, smart phones
* iPads, electronic devices of any kind
* USB drives, CDs, DVDs, and any other external storage devices

**NOTE: *if a student needs to have medication with them, please place the medication in a see through Ziploc bag to bring into the competition room.***

## Professionalism

Corporate sponsors will be observing the competition, many of whom are actively recruiting for employment. Competitors are advised to dress appropriately, use professional language, and practice good hygiene.

The PRCCDC simulates a business environment with a casual dress code. "Casual dress" means you should dress comfortably, as long as you still look dressed for work. For example, clothing that you would wear exercising, going to the beach, or going to a dance club isn't suitable for the workplace or the PRCCDC. Competitors are permitted to wear comfortable, informal clothing as long as it is not distracting or offensive to others. Suggested options for both men and women include jeans, casual slacks, polo shirts, button-down shirts, and nice t-shirts. Women may wear informal blouses and skirts as well, as long as they are an appropriate length. Although comfort is a priority, clothing must still be work-appropriate and professional. Clothing that reveals too much cleavage, your back, your chest, your stomach, or your underwear is not appropriate. Examples of casual dress attire can be found at <http://humanresources.about.com/od/dresscodesforwork/ig/Casual-Dress-Code/>

## Scoring Overview

PRCCDC scoring is based on four main components:

* **Availability:** Maintaining functionality of required services throughout the competition
* **Injects:** Completing business tasks assigned by the White Team
* **Attacks:** Preventing unauthorized access by the Red Team
* **Incident Reports:** Documenting and remediating any successful Red Team attacks

The components for availability, injects, and incident reports contribute positive points to the team's final score; attacks reduces the team's final score. As maintaining functionality of required service is as important as completing business tasks, availability and injects are weighted equally.

**At no time will questions about the status of the team's services or the team's current score be answered.** Teams are expected to monitor their own performance throughout the competition.

**Teams may verify that their business injects were received on time. This is the only item that can be challenged.**

## Availability Scoring

Certain required services (e.g., e-mail, web, database) are expected to be operational at all times throughout the competition. In addition to accepting connections, the services must be functional and serve their intended business purpose. Service availability is measured at random intervals by an automated Scoring Engine. The list of required services will be provided at the start of the competition.

Missing or misconfigured DNS records can negatively affect availability scores. The team's authoritative DNS server is used to determine the location of required services, so it is important to ensure DNS records are kept accurate and available during the competition.

Failure to document password changes can negatively affect availability scores. Additionally, the team must document all password changes for required services. Depending on the service being checked, the Scoring Engine may simulate logging in as one of the team's user accounts. The proper procedures for submitting password changes will be provided at the start of the competition.

## Inject Scoring

Throughout the competition, the White Team will assign teams to complete business tasks known as injects. Injects vary in nature and points will be weighted based upon their difficulty, criticality, and urgency.

Examples of injects used in past competitions include:

* Formulate a corporate policy to address the use of social networking
* Rebrand the company's web site including all text, images, logos, and domain names
* Create new users and groups with specific permissions
* Setup an FTP service for 2 hours with a given username and password
* Install a given software package on the CEO’s desktop
* Block specific ports, protocols, or IP addresses at the network perimeter

Injects may be scored by rank ordering the team's performance against all competitors, may be scored as pass/fail with points awarded on an all-or-nothing basis, or may contain multiple parts with points awarded for the completion of each part. It is important to complete each inject before the associated deadline as no points will be awarded for late injects. However, it may be worth your while to complete an inject after the deadline has passed (for no additional points) because many injects build upon each other.

Each team with have one or more dedicated judges assigned by the White Team. During the competition, these team judges will answer clarifying questions about injects and competition rules. If needed, the team judges will consult the White Team Room Leaders and ultimately the White Team Captain. The White Team Captain has final authority on all questions and decisions.

## Inject Time Management

The White Team may give competitors the option of working on certain business tasks outside of the official competition hours. For example, an inject assigned on the first day of the competition may be due at the start of the second day. The business tasks for these multi-day injects are general in nature and can be completed without access to the competition environment. To avoid missing the deadline and scoring zero points for these injects, competitors are strongly encouraged to submit them either before the end of the first competition day or during their spare time between the two competition days.

Any team planning to take advantage of the opportunity to work on injects after hours has the responsibility to secure access to an Internet-connected computer between the two competition days. The Seattle Airport Marriott and other hotels offer free wireless Internet access in the hotel lobby as well as a full-service business center with computers for guest use, although the availability of these services cannot be guaranteed. **In no case will competitors have access to the PRCCDC competition environment or computing resources outside of the official competition hours.**

## Attack Scoring

The attacks component, which measures successful penetrations by the Red Team, reduces the team's final score. Red Team actions are cumulative, with only the highest level of compromise scored for each attack. The point deduction for a particular attack is based on three factors:

* The criticality of the affected device (e.g., attacks against the Domain Controller result in a larger penalty than attacks against a workstation)
* The level of compromise (e.g., root-level access results in a larger penalty than user-level access)
* The method of attack (e.g., password guessing attacks result in a larger penalty than buffer overflow exploits)

Examples of successful Red Team actions that may result in point deductions for the team include:

* Obtaining user-level or administrator-level (root) access to a team's system
* Recovering account credentials (usernames and passwords, in encrypted or unencrypted form)
* Recovering critical information from a team system (configuration files, corporate data, personally identifiable customer information, etc.)
* Defacing the team's company web site
* Manipulating the team's databases

## Incident Reporting

To reduce the penalty for a particular attack, the team may submit an Incident Report contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access or information obtained, damage done, etc.), a discussion of what was affected, and a remediation plan. A thorough Incident Report that correctly identifies and addresses a successful Red Team attack may reduce the penalty for that particular event by 50%. No partial points will be given for incomplete or vague Incident Reports. The proper procedures for submitting Incident Reports will be provided at the start of the competition.

# CCDC National Competition Rules

The following are the national rules for the 2014 CCDC season. PRCCDC has local competition rules unique to this specific competition. The local variations described earlier this packet **supersede** any conflicting national rules listed below.

## Competitor Eligibility

1. Competitors in CCDC events must be full-time students of the institution they are representing.
   1. Team members must qualify as full-time students as defined by the institution they are attending.
   2. Individual competitors may participate in CCDC events for a maximum of five seasons.  A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event.  Participation on a team in any CCDC event during a given season counts as participation for that entire season.
   3. A competitor in their final semester or final two quarters prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.
   4. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.
2. Competitors may only be a member of one team per CCDC season.

## Team Composition

1. Each team must submit a roster of up to 12 competitors to the competition director of the first CCDC event they participate in during a given CCDC competition season.  Rosters must be submitted at least two weeks prior to the start of that event.  All competitors on the roster must meet all stated eligibility requirements.  No changes to the team roster will be permitted after the team competes in their first CCDC event.  The competition team must be chosen from the submitted roster.   A competition team is defined as the group of individuals competing in a CCDC event.
2. Each competition team may consist of up to eight (8) members chosen from the submitted roster.
3. Each competition team may have no more than two (2) graduate students as team members.
4. 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.
5. Once a CCDC event has begun, substitutions or additions of team members are prohibited.  A team must complete the competition with the team that started the competition.
6. ﻿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.
7. 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.
8. An institution is only allowed to compete one team in any CCDC event or season.

## Team Representatives

1. Each team must have at least one representative present at every CCDC event.  The representative must be a faculty or staff member of the institution the team is representing.
2. Once a CCDC 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).
3. Representatives may not enter their team’s competition space during any CCDC event.
4. Representatives must not interfere with any other competing team.
5. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance or red team functions, with their team during CCDC competition hours and must not attempt to influence their team’s performance in any way.

## Competition Conduct

1. Throughout the competition, Black Team and White Team members will occasionally need access to a team’s system(s) for scoring, troubleshooting, etc.  Teams must immediately allow Black Team and White Team members’ access when requested.
2. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by White Team members.
3. 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.  All hardware related questions and issues should be referred to the White Team.
4. Teams may not remove any item from the competition area unless specifically authorized to do so by White Team members. This includes items brought into the team areas at the start of the competition.
5. Team members are forbidden from entering or attempting to enter another team’s competition workspace or room during CCDC events.
6. 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).  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.
7. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
8. 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.
9. Team members will not initiate any contact with members of the Red Team during the hours of live competition.  Team members are free to talk to Red Team members during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.
10. Teams are free to examine their own systems but no offensive activity against other teams, the Black Team, the White Team, or the Red Team will be tolerated.  This includes port scans, unauthorized connection attempts, vulnerability scans, etc.  Any team performing offensive activity against other teams, the Black Team, the White Team, the Red 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 actions can be considered offensive in nature contact the White Team before performing those actions.
11. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity.  Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.  Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
12. All team members will wear badges identifying team affiliation at all times during competition hours.

## Internet Usage

1. Internet resources such as FAQs, how-tos, existing forums and responses, and company websites, are completely 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 are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted.  Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.
2. 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, 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 is prohibited unless the environment was provided by and is administered by competition officials.  Accessing private staging areas is grounds for disqualification and/or a penalty assigned to the appropriate team.
3. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.
4. Internet activity, where allowed, will be monitored and any team member caught 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 AIM/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.
5. All network activity that takes place on the competition network may be logged and subject to release.  Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

## Permitted Materials

1. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition 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.
2. 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 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.
3. 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.

## Professional Conduct

1. All participants, including competitors, coaches, White Team, Red Team, and Black Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.
2. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.
3. All CCDC events are alcohol free events.  No drinking is permitted at any time during competition hours.
4. Activities such as swearing, 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.
5. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
6. Competitors behaving in an unprofessional manner may receive a warning 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 CCDC competitions for a period of no less than 12 months from the date of their expulsion.
7. 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.

## Questions, Disputes, and Disclosures

1. PRIOR TO THE COMPETITION: Team captains are encouraged to work with the Competition Director and their staff to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.
2. 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.
3. 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.
4. 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.
5. All competition materials including injects, scoring sheets, and team-generated reports and documents must remain in the competition area.  Only materials brought into the competition area by the student teams may be removed after the competition concludes.

## Scoring

1. Scores will be maintained by the White Team and may be shared at the end of the competition.  There will be no running totals provided during the competition.  Team rankings may be provided at the beginning of each competition day.
2. Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score.  Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should immediately contact the competition officials to address the issue.