

Information:

Drawer: Accounts Payable - Invoices

Vendor Number: 1541361

Vendor Name: Parker B. Flannery

Invoice Number: 031920

Invoice Date: 03/19/20

PO Number:

Check Number: 0266621

Check Amount: \$ 125.00

Check Date: 04/14/2020

Department ID: 02736

Reviewer Name:

Voucher Number: V0617601

Redaction Type: FERPA

Document Type: AP Invoice-3 Way/Pre-Approved

Document Below

-----  
From: acctpay@cod.edu  
Sent: Mon Apr 13 10:51:37 CDT 2020  
To: invoicing@cod.edu  
CC:  
Subject: FW: Check request forms for GenCyber Camps  
-----

**From:** Landers, Susan <landerss@cod.edu>  
**Sent:** Monday, April 13, 2020 10:02 AM  
**To:** Accounts Payable <acctpay@cod.edu>  
**Cc:** Ho, Ben <hob@cod.edu>  
**Subject:** Check request forms for GenCyber Camps

Hello, attached please find check requests for non-employees who helped us with an on campus event on March 7.

Will these checks be mailed since we will not be returning to campus for awhile yet? Please let me know, thank you.

Susan Landers  
Manager, Learning Technologies  
(630) 942-2351  
LandersS@cod.edu  
<http://www.codlearningtech.org/>

**College of DuPage**  
425 Fawell Blvd  
Glen Ellyn, IL 60137  
Follow us on Twitter | Like us on Facebook

College of DuPage - Accounts Payable  
Check Request Form  
revised 11/20/19

This form may be used to request check payments **only for those items for which the issuance of a purchase order would not be appropriate**. Attach supporting documentation (e.g., invoice or agreement). Please refer to Vendor Payment - Non-Purchase Order Procedure No. 10-65

Date: 3/19/2020  
Vendor ID: [REDACTED]

Invoice Number	Fund	Func.	Dept.	Object	Object Descrip.	Amount
See grant proposal	06	10	02736	5309001	Other Contractual Services Exp	\$ 125.00
Grand Total						\$ 125.00

Check the appropriate box below and sign

- ☒ We, the undersigned, hereby certify that the goods/services for which payment is herein requested, have been provided in a satisfactory condition/manner. Consequently, payment is appropriate at this time.
- ☐ We, the undersigned, hereby certify that the goods/services for which payment is herein requested have not yet been provided. The first approver indicated below will notify the Accounts Payable Office in writing when the goods/services have been delivered in a satisfactory condition/manner.

Payee Name:

Other  
Instructions:

Payee Address:

Description on Check:

Student Mentor for GenCyber Follow-Up event March 7, 2020

Approvals:

Prepared By: Diana Kiabi

Approved By: Susan Landers

Date: 3/19/20

Signature:

Signature: Susan Landers

Payment Due:

Approved By: Kirk Overstreet

Date: 4/9/2020

Board Approved Date:

Signature:

Approved By Division VP:

Date:

Signature:

Mark Curtis-Chavez

4/10/2020

Return Approved Request and All Supporting Documents to: Accounts Payable (SRC 2132 A), [acctpay@cod.edu](mailto:acctpay@cod.edu)

**TABLE OF CONTENTS**  
**GenCyber Cybersecurity Camps**  
**College of DuPage 2019 Student Camp Grant Proposal**

<b><u>SECTION I</u></b>	<b><u>1</u></b>
<b>PROGRAM OVERVIEW</b>	<b>1</b>
<b>IMPLEMENTATION</b>	<b>5</b>
<b><u>SECTION II</u></b>	<b><u>5</u></b>
<b>TARGET PARTICIPATION</b>	<b>5</b>
<b>RECRUITMENT</b>	<b>6</b>
<b>ENROLLMENT</b>	<b>6</b>
<b><u>SECTION III</u></b>	<b><u>6</u></b>
<b>LEARNING</b>	<b>6</b>
<b>ASSESSMENT – CONDUCT PERFORMANCE-BASED ASSESSMENTS</b>	<b>7</b>
<b>PROGRAM LEGACY</b>	<b>8</b>
<b>GENCYBER CURRICULA DELIVERY</b>	<b>8</b>
<b>REFLECTION</b>	<b>8</b>
<b><u>SECTION IV</u></b>	<b><u>10</u></b>
<b>PROGRAM PERSONNEL</b>	<b>10</b>
<b>FACULTY QUALIFICATIONS</b>	<b>10</b>
<b><u>SECTION V</u></b>	<b><u>12</u></b>
<b>SUMMARY</b>	<b>12</b>
<b>REFERENCES</b>	



**College of DuPage 2019 GenCyber Student Camps****Proposal Narrative****Section I: Program Overview/Introduction****A. Program Overview**

College of DuPage (COD), Glen Ellyn, IL, serves approximately 27,000 highly diverse, traditional and non-traditional students each semester on the second largest provider of undergraduate education in Illinois. COD has a well-developed infrastructure, deep academic expertise, and significant academic and industry relationships. The Center for Cyber Defense Education at COD is dedicated to the development, promotion and support of education, collaboration and innovation in security technologies and management, information security assurance and digital forensics across multiple academic and professional disciplines. The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated College of DuPage as a National Center of Academic Excellence in Cyber Defense Two-Year Education (CAE-CDE 2Y). Students in the cybersecurity program at COD earn a two-year associate's degree in the Cybersecurity discipline and are able to sit for seven different industry certification exams. The college regularly sponsors cybersecurity-related community events such as cybersecurity education workshops, camps and summer programs, state Homeland Security trainings, First Responder workshops and computer diagnostic check-ups. Students and faculty also participate in many regional and national cybersecurity competitions.

Statistics demonstrate that the graduation rate of students with cybersecurity majors is not keeping pace with the demand for talent in the workplace. It is predicted that 1.8 million more cybersecurity professionals will be needed to meet the occupational demand by 2022 (Center for Cyber Safety and Education (CCSE, 2017). The federal government also recognizes the impending crisis, especially within governmental institutions. A recent report to the White House (U.S. Secretary of Commerce and US Secretary of Homeland Security, 2018) advises the importance of aligning education and training with employer's workforce needs in order to facilitate the pathway from classroom to workroom. In response, COD proposes hosting two week-long GenCyber Student Camps, to be held in Summer 2018. The first week is designed specifically for students of grades 6-9 and the second week is dedicated for students in grades 7-12. Curriculum will center on teaching First Principles of cybersecurity through hands-on exercises on real-world security issues. The camp will cover various aspects of cybersecurity and participants will learn about privacy, security, and safe browsing while on the Internet. Students will be introduced to cyber ethics and engaged in hands-on sessions that allow them to tackle realistic data security problems. Attendees will have opportunities to meet cyber experts and industry professionals. The camp will offer age-appropriate instructional methods to achieve these outcomes, with both sets of students also participating in detailed discussion and complex lab activities. The camp will also address career opportunities in cybersecurity fields. The camp will meet from 8:30 am to 4:30 pm each day and will provide a unique opportunity for students to learn about cybersecurity programs and to increase their overall knowledge of careers in cybersecurity. Attendees will receive a camp T-shirt, Raspberry Pi, a backpack and water bottle with the GenCyber logo, and materials with various activities related to the GenCyber Cybersecurity First Principles.

Safety of the students is a priority. All staff will attend precamp training and orientations to familiarize the new and existing staff with the GenCyber camp safety policies and procedures.

The program will use a sign-in process to maintain accurate attendance and will follow up with guardians regarding attendance issues. An 8:1 student-staff ratio will be maintained and students are supervised and escorted when needing to leave the classroom. In the interest of safety, students and staff will wear identification that indicates they are part of the GenCyber Camp.

The curriculum will facilitate a learner-centered classroom by focusing on appropriate teaching strategies and hands-on activities for each age group. Project Personnel will use their expertise to ensure that the principles of cybersecurity are presented and practiced by participants through interactive activities that reinforce retention of essential information. The use of the Raspberry Pi during the hands-on activities and the ability of the students to keep that technology after the camp is completed will contribute to the learner-centered approach of these activities.

### **College of DuPage GenCyber Student Camp 2019 Curriculum and Implementation**

The camps will implement a curriculum that employs active learning strategies centered on GenCyber Cybersecurity First Principles. This curriculum has been successfully applied in previous GenCyber student and teacher camps. Cybersecurity First Principles are introduced during the first day of camp with final activity of the first day being the “First Principle Challenge Course” that provides real-world, concrete examples of the First Principles. Throughout the week, First Principles are reinforced through a variety of explicitly chosen lessons for students to develop their conceptual foundation of cybersecurity. To enhance learning, applicable lessons are integrated or linked with previous modules to help students make connections and reinforce the knowledge.

<b>FIRST PRINCIPLE:</b> Resource Encapsulation, Modularity, Least Privilege, Abstraction, Process Isolation, Layering	
<b>UNIT:</b> Cyber Crime, Social Engineering, Ethics and Trends	
<b>Learning Objective</b>	Demonstrate and describe the importance of safe online behavior to others; Illustrate the implications of unsafe online behavior
<b>Topic Outline</b>	Human behavior as an aspect of cybersecurity; Online safety in social media, cyberbullying, sexual predators, and identity theft; Hacking techniques
<b>Activities</b>	Small group activity and discussion; Interland online game; Review of Ethics and Law case study

<b>FIRST PRINCIPLE:</b> Resource Encapsulation, Modularity, Least Privilege, Abstraction, Process Isolation, Layering	
<b>UNIT:</b> Intro Cybersecurity, Cybersecurity Awareness	
<b>Learning Objective</b>	Define the technical aspects of cybersecurity to students; List steps to personal online protection and translate them to students; Name basic cybersecurity skills and identify defensive strategies.
<b>Topic Outline</b>	Current trends and crime case studies; Fraud, scams, phishing, ransomware, digital evidence
<b>Activities</b>	Identity theft exercise and/or witness a mock crime as a team and report observation to a detective; Digital forensics evidence collection; Discuss safe online behavior in small groups

<b>FIRST PRINCIPLE:</b> Resource Encapsulation, Modularity, Least Privilege, Abstraction, Process Isolation, Layering		
<b>UNIT: Computer Raspberry PI</b>		
<b>Learning Objective</b>	Basic computer components and how they relate to security and the internet; Demonstrate assembly of a small computer for students; Set up computer assembly lab; Introduction to coding concepts using Raspberry Pi computers	
<b>Topic Outline</b>	Domain Separation; Computer parts; Security hardening of operating systems and applications	
<b>Activities</b>	Building a computer; Configure operating system, networking & web browser security settings; Set up different layers of user account; Update & coding of Raspberry Pi; Small group discussion on the use of Raspberry Pi computers; Raspberry project video; Age-appropriate online cyber security games	

<b>FIRST PRINCIPLE:</b> Minimizations, Modularity, Least Privilege, Process Isolation, Layering		
<b>UNIT: Networking Fundamentals</b>		
<b>Learning Objective</b>	List and explain networking and firewall design principles concepts	
<b>Topic Outline</b>	Basic firewall rule configuration (Authentication, Authorization, and Accounting); Access control; System and security logging; Firewalls, firewall policies and layering network security; TCP/IP concepts; Protection mechanism; Host Intrusion Detection	
<b>Activities</b>	Host intrusion detection; Access control testing; Configure and test network and firewall configurations using Raspberry Pis; Internet of Strings & Pirate Islands; ASCII conversion; IP addressing; Video: Warriors of the Net	

<b>FIRST PRINCIPLE:</b> Domain Separation, Least Privilege		
<b>UNIT: Credentials</b>		
<b>Learning Objective</b>	Demonstrate cybersecurity protection mechanisms through the use of credentials and explain significance of credentialing; Discuss limitations of typical password schemes and model effective password selection	
<b>Topic Outline</b>	Security Design Principles: domain separation, least privilege, process isolation, password creation and protection; Browser configuration and security web-based attacks; Cross-site scripting; URL masquerade attack; Session hijacking	
<b>Activities</b>	Password Creation project; Group Discussion on credentials and attack methods; TEDTalk Video: How to use Passwords & Be Safer Online	

<b>FIRST PRINCIPLE:</b> Least Privilege, Minimization, Simplicity		
<b>UNIT: Vulnerabilities</b>		
<b>Learning Objective</b>	Distinguish and articulate system and software security threats and vulnerabilities; Perform penetration testing of systems and recommend remedial actions for system hardening.	
<b>Topic Outline</b>	Security auditing software; Vulnerability scanning software; Penetration testing tools; Security auditing; Vulnerability assessment; System and application hardening	
<b>Activities</b>	Discussion of security testing; Cybersecurity Card Games; Demonstration of Man in the Middle; credential capturing using Wireshark; PBS Nova Cybersecurity Labs online game; Demonstration of Session Hijacking; Online cybersecurity simulation games	

<b>FIRST PRINCIPLE:</b> Data Hiding		
<b>UNIT: Cryptography</b>		
<b>Learning Objective</b>	Recall basic cryptographic concepts, analysis, techniques, and tools and synthesize them for students; Discuss and explain applications of cryptography in cyberspace.	
<b>Topic Outline</b>	Cryptography concepts, theory, and techniques; Symmetric and asymmetric encryption Caesar, ROT and Vigenere ciphers; Public key cryptosystems Information Hiding Protocols concepts and techniques of steganography; Digital signature and certificates; File, directory, and email encryption	
<b>Activities</b>	Watch and discuss: NOVA PBS Cyber Codes video; Caesar and Vigenere samples; Demonstration: Steganography; Kiddie-RSA-working with module arithmetic Play and demonstrate information hiding protocol games; Key exchange; Data error checking; Solve zero knowledge proof puzzle and explain solution process to students; Visit cryptology websites and participate in code breaking challenges individually and as groups.	

<b>FIRST PRINCIPLE:</b> Domain Separation, Process Isolation, Layering, Simplicity		
<b>UNIT: Risk</b>		
<b>Learning Objective</b>	Illustrate risk management concepts in cyberspace; Perform a basic risk assessment and analysis; Discuss risk treatment options.	
<b>Topic Outline</b>	Cybersecurity risk concepts, risk assessment and analysis; Risk treatment options: mitigation, transference, acceptance; Cyber Threats and vulnerabilities; Associated problem-based laboratory	
<b>Activities</b>	Group discussion of best practices associated with cybersecurity risks, including physical security, wireless technologies and information security; Simple case study on a hypothetical business' IT risk assessment and analysis; Group discussion on risk treatment options and their applicability on specific cases; Facilitate consumer protection video discussion; Facilitate role playing using online cyber-criminal activity	

<b>FIRST PRINCIPLE: All</b>		
<b>UNIT: Forensics, Cyber Crime Simulation</b>		
<b>Learning Objective</b>	Identify cybersecurity threats and risks during a simulation; Apply appropriate responses at each step of simulation; Evaluate effectiveness of responses	
<b>Topic Outline</b>	Law enforcement; Incident Response; Forensics and digital forensics; Investigation and evidence collection; Social media; Computerized intelligence databases and resources; Computer fraud; Middleman scams; Wire fraud; Sexual predator investigations, sexting and cyberbullying	
<b>Activities</b>	Comprehensive simulation activity designed to help apply the learned concepts; Discuss and research several methods of obtaining evidence by searching the internet and email; Tracking internet protocol addresses; Exploiting intelligence databases and social networks including searching computers, cell phones and electronic media; Deciphering computer data; Group discussion of the legal process such as search warrants and subpoenas	

## **B. Implementation**

COD has extensive experience and a strong reputation for providing high-quality professional development for adults, including teachers. The GenCyber Teacher Camp curriculum is developed and implemented by professors in the COD Computer and Internet Technologies Department in collaboration with members of the Homeland Security staff. The combined expertise of the facilitators will ensure the quality and viability of the teacher camps, and that the NSA GenCyber learning objectives are met. The COD campus has the classroom and meeting room space and other facilities necessary for all camp activities. COD will also utilize the Homeland Security Training Center venue that is a dedicated first-responders facility housing the college's Criminal Justice, Fire Science/EMS, Police Department and the Suburban Law Enforcement Academy. Food service for the camp will be provided for the camps on-site, and the COD Grants Office will assist as necessary in overseeing program activities and ensuring the goals of the grant program are met.

## **Section II: Target Participation/Recruitment/Enrollment**

### **II-A. Target Participation**

The COD GenCyber Student Camp will be offered to students entering sixth through twelfth grade from the 38 communities served by the college and the surrounding Chicago metropolitan area. These communities are highly diverse, representing a rich mix in culture, ethnicity, socioeconomic status, educational attainment, and technological expertise. Camp staff will strive to ensure that the group of students enrolled in the camp is also diverse, and that whenever possible, they represent an equal gender mix; diversity in culture, ethnicity, and socio-economic status; and a variety of levels of cybersecurity expertise and computer knowledge. The camp will serve students through a range of age-appropriate activities designed to increase participants' knowledge of safe online behavior, GenCyber First Principles and careers in cybersecurity.



## **II-B. Recruitment**

COD will publicize the GenCyber 2019 Student Camp through targeted brochures and informational flyers distributed directly to the schools within the county. Emails with marketing materials will be sent to participants of the 2017 and 2018 Teacher and Student Camps as well as students who have expressed interest and are currently on a waitlist for a potential 2019 GenCyber Student Camp. Camp staff will host a booth at STEM-CON, a free interactive fair hosted by College of DuPage that is attended by over 2,000 people of all ages who can engage in hands-on exhibits, exclusive speakers and informative demonstrations on many STEM fields (<http://www.cod.edu/stemcon>). At the fair, staff will hand out informational brochures and puzzle giveaways with the GenCyber logo. Information about the program will also be distributed through the through public service announcements on the college radio station, WDCB, posters on campus, and notifications on the electronic signage around the main campus and the five additional regional College of DuPage campuses throughout the district.

## **II-C. Enrollment**

The COD GenCyber Student Camps will limit enrollment to 36 students for each of two weeks of camps (72 total participants) for appropriate instructor-participant ratio, suitable sizing for pairing and small group activities and adequate fit in the campus facilities. Applicants will come from regional middle and high schools. Given the success of prior College of DuPage GenCyber Student Camps, a list of students who are interested in participating in a camp for 2019 has been initiated. Recruitment and enrollment efforts will begin upon notification of funding, and all promotional efforts will highlight the integration of technology and hands-on experiences as a means of attracting highly motivated STEM students who are excited about learning more about cybersecurity and careers within that field. To ensure a diverse cohort of participants, enrollment will occur through a weighted lottery system in order to achieve equal gender, ethnicity, school community, and cultural diversity among the participants. Planning and preparation by the program staff will focus on developing fun and engaging activities that will demonstrate and reinforce the principles of cybersecurity that are a part of this program in ways that capture a student's interest and desire to learn more.

## **Section III: Learning/Assessment/Legacy/ Curricula Delivery/Reflections**

### **III-A. Learning**

Instruction at the Student Camps will include a blend of lecture, demonstrations, interactive exercises, and other activities that will assist student participants to understand and learn the ten Cybersecurity First Principles, and in addition will model for them ways they may share this content with others. It is anticipated that about 30 hours of the time will be spent in instructor-led lecture, demonstration or exercises, and the remaining time will be spent with activities that include working through cybersecurity-related exercises, learning via cybersecurity-related games and interactive quizzes, and developing projects they can share with others after the conclusion of the camps. Cybersecurity concepts will be demonstrated through the following activities:

- COD faculty, staff and students sharing related projects
- Guest speakers from industry and government
- Faculty-led tours of the college's STEM facilities, Cybersecurity and Homeland Security training facilities (approximately one hour)
- Cybersecurity scavenger hunt capstone activity (4 hours)

Students will also spend a minimum of one hour per day developing cybersecurity awareness material based on each day's activities. Participants will be introduced to online cybersecurity games, that will be used to help reinforce cybersecurity concepts during the camp and outside the camp. Students will create and share projects that demonstrate safe online behavior or one of the GenCyber First Principles that they can take with them to help spread cybersecurity awareness to others. The curriculum for the 2019 GenCyber Student camps will closely follow the 2018 curriculum, with improvements incorporating the feedback from 2018 participants and Site Visitors. These include stating learning objectives at the beginning and re-capping them at the end of each lesson to help students better understand the purpose of each lesson. More time will be allocated during the day for students to work on activities in pairs and small groups, to encourage learning at a greater depth with each activity. Students will be required to have an email account prior to the start of camp in order to explore the cybersecurity websites that are part of the camp lessons. All software installations and downloads will be achieved prior to camp in order to maximize camp time for instruction. Finally, teachers from previous COD GenCyber Teacher camps will assist the students in developing their cybersecurity projects to ensure students understand the expectations.

### **III-B. Assessment**

#### **1. Process**

Program staff will develop pre- and post-course surveys to assess student cyber knowledge and learning outcomes, and the post-course survey will also measure student satisfaction with the overall camp experience and specific learning activities or other camp components. Short daily surveys will assess day-to-day growth. This information will be used in the planning of future camps or other offerings pertaining to cybersecurity by the college. Progress made by students in simulations will be recorded for overall assessment of learning outcomes. Participant achievement will be evaluated through successful participation in and completion of various activities. Participants will receive immediate feedback from instructors regarding their progress during the activities throughout the course. At the end of the course, students will participate in a simulation that provides them an opportunity to apply the concepts learned throughout the week. A variety of activities will be used to meet the needs of diverse learners with different learning styles: lecture, discussions in both large group and small group format, evaluation of case studies and hands-on activities such as building a mini computer.

#### **2. Feedback**

Participants will be provided with formative oral feedback by the instructors throughout the camp to ensure their engagement and ongoing learning. Participant feedback is vital to the success of the program. Satisfaction surveys will be conducted at the end of the camps. Responses will use a 5-point Likert scale to assess the perceived level of engagement during the camp, as well as the level of acquired level of comprehension of online safety and cybersecurity.

#### **3. Reflection opportunities**

Each day will begin with informal discussions of the previous days' topics, which will be followed by an informal assessment of the previous days' topics. Based on these exercises, the instructor will be able to assess if the previous teaching strategies were successful and if topics

needs additional instruction time. At the end of each day, they will be asked to do a simple exercise, such as completing a prompt, to reflect on their learning and to share with others something new that they learned that day. In addition, students will be asked to provide a peer critique of each other's cybersecurity projects.

#### **4. Diversity**

The camps will comprise a diverse group of students, with each bringing their own individual backgrounds, sets of skills and knowledge. The participants will interact with each other including observation and collaboration on curriculum, which will allow for sharing of their diverse backgrounds. Group formation will be guided by instructors in order to encourage diversity within each group. By providing Raspberry Pis, participants will have access to technology in their home. The program will also address diversity by supplying a varied set of instructors and guest speakers.

#### **III-C. Program Legacy**

During the camp, students will create cybersecurity awareness materials that will be shared via group presentations and COD events. In conjunction with the Department of Homeland Security's Cyber Security Awareness month in October, COD GenCyber project staff will promote awareness through a series of email communications to past GenCyber participants of activities and other cybersecurity informational resources. COD GenCyber Program Staff will also serve as resources for students who desire to start cybersecurity clubs at their own schools. COD GenCyber Program staff will maintain communication with camp participants to share additional cybersecurity education opportunities that are available on campus and in the community such as COD Youth Education, STEMCON, and local events.

#### **III-D. Curricula Delivery**

Student participants will form cohorts to create age-appropriate cybersecurity awareness materials on the topics covered each day. Students will have several opportunities for collaboration such as team building activities, participation in a cyber crime simulation at the end of the camp, and development of cybersecurity awareness materials. Reliable and readily available technology will be used to support the learning goals including Raspberry Pi's, Chromebooks, Makey Makey devices and Ozobots.

#### **III-E. Reflections from 2018**

The site visit report for the College of DuPage 2018 GenCyber Student Camps was overall very positive but did note a few recommendations to incorporate in future camps, including:



<b><u>CONCERN</u></b>	<b><u>RECOMMENDATION</u></b>
Participants may have difficulty seeing demonstrations at the front of the room.	The use of a document camera during any class demonstration will assist in providing visual instruction for all students in the classroom, regardless of where they sit. Where applicable, live demonstrations will be adjusted for presentations in smaller groups or projected pre-recorded video will be used. Guest speakers and instructors will also be made aware of classroom features, such as document cameras, microphones and interactive display tools.
Cybersecurity skills and knowledge are better taught and reinforced through a pre-learning method rather than just beginning the class directly with instruction.	The day's objectives will be posted at the beginning of each day. A pre assessment using iClickers will be given, which will contain pre-learning questions relating to the day's activities. Each lesson and activity will be begin by presenting the learning outcome both verbally and visually to prepare the student for active learning.
K-12 teacher was not fully engaged in the camp experience.	K-12 teacher coach(es) will be used more effectively during precamp planning as well as during implementation of the camp. A formal precamp staff orientation process will ensure that each staff member understands their role and the necessary responsibilities and requirements to run a successful camp.
There was a predominance of boys in both camps. The girls who were present at the camps tended to stay together rather than joining other groups of boys in the camp.	Edit the camp application to include gender and utilize a weighted lottery system to ensure an even distribution of both boys and girls in the camps. Whenever possible, mindfully group the students to create an equal distribution of gender and other attributes across groups.
It was good to establish classroom rules and policies at the beginning but they need to be conveyed both verbally and visually to accommodate all learners.	Classroom "Rules of the Road" (rules and policies) are created on the first day of each camp interactively with the student participants. The "Rules of the Road" will be posted in each classroom as a visual reminder of classroom rules and regulations for student campers.

Utilizing a K-12 Curriculum Development Specialist to review curriculum and suggest age-appropriate activities was found to be a strong factor of the success of the College of DuPage GenCyber Student Camps. Although it is not a mandatory requirement for teachers who participated in our teacher camp, having many teachers from the Teacher Camps return to assist with the activities and teach a few lessons also made the camp experience more engaging and impactful for the students. Family engagement was also a positive result of the 2018 GenCyber Student camps as parents came to observe student presentations of their GenCyber-related projects at the conclusion of camp.

## **Section IV: Program Personnel and Faculty Qualifications**

### **IV-A. Program Personnel**

COD is uniquely qualified with unprecedented opportunities for interdisciplinary educational and professional projects and collaborative experiences across a variety of computer and criminal justice and security disciplines. The Center for Cyber Defense Education at College of DuPage is dedicated to the development, promotion and support of education, collaboration and innovation in security technologies and management, information security assurance and digital forensics across multiple academic and professional disciplines.

The Homeland Security Training Institute (HSTI) at College of DuPage develops and delivers cutting-edge training and comprehensive programming that is reshaping American public safety and emergency response. HSTI leads at the local, regional and national levels through content experts at the top of their fields, state-of-the-art facilities and equipment, and innovative curriculum. The Computer and Informational Technologies (CIT) program at College of DuPage offers a variety of degrees and certificates that allow graduates to pursue a career in a wide range of information technology fields. In addition, CIT offers several certification training programs through its Microsoft Academy, Cisco Networking Academy and the CompTIA Academy. The CIT and HSTI specialists will develop the curriculum and provide instruction for the camp. A variety of subject matter experts will present on aspects of cybersecurity.

**Justin Wagner, Instructional Lead** (Associate Professor, College of DuPage). Mr. Wagner has worked in the IT industry for over 20 years, primarily in K-12 environments. Justin has been the mentor for high school student IT clubs, a middle school basketball coach and currently volunteers his time helping financially-struggling schools. As a college-level instructor since 2000, has also helped to develop and teach cybersecurity courses at the COD. He holds numerous Cisco and CompTIA certifications.

**Julie Konczyk, Project Director** (Continuing Education Program Manager, College of DuPage) Ms. Konczyk is Program Manager for the Youth Academy and Adult Enrichment at COD. She has an M.A. in Anthropology and has been developing credit and non-credit courses for over 10 years, including assisting faculty in the transition of face-to-face curriculum into online modalities. She will be responsible for marketing, enrollment, recruitment and day-to-day logistics.

### **IV-B. Additional Faculty Qualifications**

**Tony Chen, Instructor** (Professor, College of DuPage). Mr. Chen received his master's degree in computer science from the Illinois Institute of Technology. He developed the cybersecurity degree at COD and has taught most of the courses in this degree. He holds Cisco CCNA certifications, CompTIA certifications, and Microsoft Certified Solutions Associate certification for Server 2012. Tony will assist in the curriculum design process including lesson plans, activities, objectives, delivery of instruction and participant assessment.

**Tom Brady, Instructor** (Associate Dean, Homeland Security Training Institute, College of DuPage) Mr. Brady holds a MSc. in Integrated Homeland Security Management. Tom served as the Inspector in Charge of the Chicago Division with the US Postal Inspection Service from

May, 2007 until March, 2013. He has provided executive oversight for his former agency in two significant investigations: The Amerithrax (anthrax) investigation in Washington DC, and the former Governor Rod Blagojevich investigation in Chicago.

**Jennifer Fowler, Instructor** (Cybersecurity Analyst, Cyber Operations, Analysis, and Research, Argonne National Laboratory) will lecture on her career path in becoming a Cyber Security Analyst at Argonne National Laboratory, her role in Argonne's Cyber Defense Competition and promoting Cyber Security education. Jennifer is the author is on numerous puzzles used by Argonne's Department of Energy CyberForce Competition (<https://cyberforcecompetition.com/>).

**Josh Norris, Instructor** (Information Technology, Community Unit School District 308) will discuss Cybersecurity, Online Safety, Cyber Hygiene with his unique perspective of a being a US Army veteran, former US Department of Defense, a retired police officer and his new career in Information Technologies for a school district with 22 schools, a 1:1 technology initiative and over 18,000 students.

**Jarret Dyer, Instructor** (Testing Center Coordinator, College of DuPage) will present on two topics: The use of "Technology and Cheating in the Classroom" and "Movies, Music and Mayhem: Protecting Intellectual Property through CyberSecurity." The two presentations will focus on how intellectual properties are protected digitally using Steganography and the real examples from his experiences overseeing Testing Services at the College of DuPage.

**Cheri Bridge, Instructor** (Technology Integration Specialist, Wilmette Public School District 39). Ms. Bridge is a Technology Integration Specialist with experience teaching elementary and middle school, staff development instructor and coach on the proper integration of technology across all content. She holds an M.A. Educational Technology, M.A. School Leadership, and is a Doctoral Candidate in Curriculum and Teaching. She holds designations as a certified Teacher Evaluator, Google Certified Educator II, Google-Digital Citizenship and Safety Recognition, and is a BreakoutEDU Authorized Trainer. Ms. Bridge has assisted schools in implementation of Illinois' standards, including ELA & Mathematics Common Core, Next Generation Science, Social Science standards, and GenCyber Principles.

**Katrina Vafakos, Site Supervisor** (Teacher, Chicago Public School District) Ms. Vafakos is a Diverse Learner Chemistry Teacher and Service Learning Coach in a Chicago-area high school. Her current focus is technology integration in the classroom, implementation of service learning projects in the classroom, and teacher mentorship. Katrina holds a M.B.A, M.S. in Information Systems, Masters in Secondary Education, Certification in School Leadership and Director of Special Education.

**Student Mentors** will be employed temporarily before and/or during the camp to facilitate program logistics and day-to-day event set-ups.

**Student Aides** will be employed temporarily during the camp to employees to assist with pick up and drop off the students, assist in the classroom and escort students to locations on campus safely.

**Section V: Summary**

Overall, the College of DuPage is dedicated to the development, promotion and support of education, collaboration and innovation in security technologies and management, information security assurance and digital forensics across multiple academic and professional disciplines. The College of DuPage's proposed GenCyber Student Camps are designed to build off that dedication. The camps' participants come from a dedicated and diverse set of applicants, who are interested in Cyber Security and the First Principles. The 2019 camps will build upon the success of the 2017 and 2018 camps and help bring a larger overall impact to middle and high school students of the Chicagoland metropolitan area.

**References**

Center for Cyber Safety and Education - Frost & Sullivan Executive Briefing. (2017). *The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk*. Accessed: <https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf>.

U.S. Secretary of Commerce and US Secretary of Homeland Security. (2018). *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*. Washington, D.C.: Government Printing Office.