

Information:

Drawer: Accounts Payable - Invoices

Vendor Number: 1494166

Vendor Name: Amber L. Krause

Invoice Number: 031920

Invoice Date: 03/19/20

PO Number:

Check Number: 0266655

Check Amount: \$ 125.00

Check Date: 04/14/2020

Department ID: 02739

Reviewer Name:

Voucher Number: V0617620

Redaction Type: FERPA

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

Document Below

From: acctpay@cod.edu
Sent: Mon Apr 13 10:51:44 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:

Invoice Number	Fund	Func.	Dept.	Object	Object Descrip.	Amount
See grant proposal	06	10	02739	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.

AP VERIFIED
04/13/20 - BETHANY CRUSE

Payee Name:

Other Instructions:

Payee Address:

Description on Check:

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

Approvals:

Prepared By: Susan Landers

Approved By: Susan Landers

Date:

Signature: Susan Landers

Signature: Susan Landers

3/19/20

Payment Due:

Approved By: Kirk Overstreet

Date: 4/2/2020

Board Approved Date:

Signature: Mark Curtis-Chavez

4/3/2020

Approved By Division VP:

Date:

Signature:

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

TABLE OF CONTENTS
GenCyber Cybersecurity Camps
College of DuPage FY19 Advanced Student Camp Grant Proposal

<u>SECTION I</u>	<u>1</u>
PROGRAM OVERVIEW	1
IMPLEMENTATION	5
<u>SECTION II</u>	<u>5</u>
TARGET PARTICIPATION	5
RECRUITMENT	6
ENROLLMENT	6
<u>SECTION III</u>	<u>6</u>
LEARNING	6
ASSESSMENT – CONDUCT PERFORMANCE-BASED ASSESSMENTS	7
PROGRAM LEGACY	8
GENCYBER CURRICULA DELIVERY	8
REFLECTION	9
<u>SECTION IV</u>	<u>10</u>
PROGRAM PERSONNEL	10
FACULTY QUALIFICATIONS	11
<u>SECTION V</u>	<u>12</u>
SUMMARY	12
REFERENCES	

College of DuPage 2019 GenCyber Advanced 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) through academic year 2022. Students in the cybersecurity program at COD earn a two-year associate's degree in the Cyber Security discipline and are able to sit for exams for seven different industry certifications. 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. In addition, students and faculty also participate in a variety of 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 1 one-week-long GenCyber Advanced Student Camp, to be held in Summer 2019. This week will be designed specifically for high school students who have participated in a prior GenCyber camp and /or have some relevant technology experience such as computer programming, networking, security, or participated in a CyberPatriot program. The camp will cover more complex topics of cybersecurity and participants will gain comprehensive in-depth knowledge regarding privacy, security, and safe browsing concepts while on the Internet. Students will be introduced to cyber ethics and will engage in interactive sessions that allow them to tackle realistic data security problems. Curriculum will be centered on teaching First Principles of cybersecurity on real-world security issues. Attendees will have opportunities to meet cyber experts and industry professionals. The camp will offer age-appropriate instructional methods to achieve these outcomes, with students also participating in detailed discussion and complex lab activities. The camp will also incorporate career opportunities in cybersecurity fields and showcase multiple

cybersecurity career pathways. 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 and interest in cybersecurity. Attendees will receive a camp T-shirt, Raspberry Pi, backpack, water bottle, and materials with various activities related to the GenCyber 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 camps, 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. Students will be supervised and escorted for any need to leave the classroom. The student to staff ratio will be a maximum of 5:1 at all times. In the interest of safety, students and staff will wear identification that indicates they are part of the GenCyber Camp. The curriculum developed during the planning portion of this program 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 in a way that will help them retain 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 centered on GenCyber Cybersecurity First Principles that has been successfully implemented using active learning strategies in previous student camps. First Principles are introduced during the first day of camp with a team bonding activity that provides real world and concrete examples of the Cybersecurity First Principles. First Principles are then reinforced through a variety of explicitly chosen lessons for students to develop their conceptual foundation of cybersecurity. Lessons are integrated or linked with previous modules to help students make connections to reinforce learning.

FIRST PRINCIPLE: Resource Encapsulation, Modularity, Least Privilege, Abstraction, Process Isolation, Layering	
UNIT: Cyber Crime, Social Engineering, Ethics and Trends	
Learning Objective	Demonstrate and explain the importance of online safety; Illustrate the implications of unsafe online behavior
Topic Outline	Human behavior as an aspect of cybersecurity; Online safety in social media; Cyberbullying; Sexual predators; Identity theft; Hacking techniques
Activities	Small group activity & discussion on ethics, social engineering, & cyber crime

FIRST PRINCIPLE: Resource Encapsulation, Modularity, Least Privilege, Abstraction, Process Isolation, Layering	
UNIT: Advanced Cybersecurity, Cybersecurity Awareness	
Learning Objective	Introduce advanced technical aspects of cybersecurity; Name cybersecurity skills; Create in-depth awareness on cybersecurity and critical thinking skills
Topic Outline	Fraud; Scams; Phishing; Ransomware; Digital evidence; Social engineering
Activities	Digital forensics evidence collection; CIA triad; Handling malware & ransomware

FIRST PRINCIPLE: Resource Encapsulation, Modularity, Least Privilege, Abstraction, Process Isolation, Layering	
UNIT: Computer Raspberry Pi	
Learning Objective	Advance computer operating system component; Operating system security settings; Set up computer assembly lab using Raspberry Pi computers
Topic Outline	Domain Separation; Linux; Security hardening of operating systems and applications; Security tools and policies
Activities	Introduction to Linux; Install and configure multiple operating systems and web browser security settings; Set up different layers of user account; Running cybersecurity utilities and software tools on Raspberry Pi

FIRST PRINCIPLE: Resource Encapsulation, Modularity, Least Privilege, Data Hiding, Minimization, Abstraction, Process Isolation	
UNIT: Coding	
Learning Objective	Introduce students to computer science and Python and Scratch programming languages; Secure coding concepts and relation to security & the internet
Topic Outline	Programming; Secure coding concepts; Python; Scratch
Activities	Create simple projects using Python and Scratch tied to First Principles concepts; Different themes and skill levels of activities will be used to engage students of varying backgrounds and interests

FIRST PRINCIPLE: Minimizations, Modularity, Least Privilege, Process Isolation, Layering	
UNIT: Advanced Networking	
Learning Objective	Explore and configure networking and firewall
Topic Outline	Advanced 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
Activities	Host intrusion detection; Access control testing; Configure and test network and firewall configurations using Raspberry Pis & Windows operating system

FIRST PRINCIPLE: Domain Separation, Least Privilege	
UNIT: Credentials	
Learning Objective	Explore cybersecurity protection mechanisms through the use of credentials; Limitations of typical password schemes; Model effective password selection
Topic Outline	Security Design Principles: domain separation, least privilege, process isolation, password creation and protection; Browser configuration and security web-based attacks; URL masquerade attack; Session hijacking
Activities	Password creation and attack project; Password attacks demonstration and mitigation technique activity; Group discussion on credentials; Exploring Session Hijacking

FIRST PRINCIPLE: Least Privilege, Minimization, Simplicity	
UNIT: Vulnerabilities	
Learning Objective	Examine system & software security threats and vulnerabilities; Perform penetration testing of systems; Recommend remediations for system hardening
Topic Outline	Security auditing software; Vulnerability scanning software; Penetration testing tools; Vulnerability assessment; System and application hardening
Activities	Use Wireshark to conduct security testing; Open source intelligence, Man in the Middle credential capturing; Nmap

FIRST PRINCIPLE: Data Hiding	
UNIT: Cryptography	
Learning Objective	Advance cryptographic concepts, analysis, techniques, and tools
Topic Outline	Cryptography concepts, theory, and techniques; Symmetric and asymmetric encryption; ROTation Cipher and Vigenere ciphers; Public key cryptosystems; Techniques of steganography; Digital signature and certificates; File, directory, and email encryption
Activities	Caesar, ROTation Cipher and Vigenere samples; Steganography; Play and demonstrate information hiding protocol games; Key exchange; Data error checking; Visit cryptology websites and participate in code deciphering challenges; Group discussion regarding cryptography and its use in society

FIRST PRINCIPLE: Domain Separation, Process Isolation, Layering, Simplicity	
UNIT: Risk	
Learning Objective	Explore risk management in cyberspace; Perform a risk assessment and analysis; Risk treatment options
Topic Outline	Cybersecurity risk concepts; Risk assessment and analysis; Risk treatment options: mitigation, transference, acceptance; Cyber threats and vulnerabilities; Associated problem-based laboratory
Activities	Group discussion of best defensive practices associated with cybersecurity risks, including physical security, wireless technologies and information security; Simple case study on a hypothetical company's IT risk assessment and analysis; Group discussion on risk treatment options and their applicability on specific cases; Facilitate "Think like an Adversary" discussion; Facilitate role playing using card games and online activities

B. Implementation

COD has extensive experience and reputation providing high-quality programming for students of all ages. The GenCyber camp described above will be created and implemented by professors in our CIT/CIS programs, in collaboration with Homeland Security staffs and the expertise of an elementary/secondary curriculum developer. The combined expertise of the facilitators will ensure the quality and viability of an advanced student camps, and that the 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 which is a dedicated first-responders facility that houses 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 throughout 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 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 further 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 (<http://www.cod.edu/stemcon>), a free interactive fair hosted by College of DuPage and 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. 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 2019 GenCyber Advanced Student Camp will limit enrollment to 20 students for the one week camp to provide a more comprehensive and in-depth cybersecurity learning experience. Applicants will come from regional high schools and must have previous experience with cybersecurity and/or relevant associated technologies. The GenCyber application will request a list previous experience with cybersecurity activities, with preference given to students who have previously attended a GenCyber Student Camp. 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 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. 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 awareness to others. The curriculum for the 2019 GenCyber Student camps will follow the 2018 curriculum, with activities that require substantially more technical proficiency. The camp curriculum will also incorporate recommendations gathered from the GenCyber 2018 camp participants and Site Visitors. These include time to explore various cybersecurity websites during the camp day. 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 project 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 need 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 curriculum.

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 beyond the summer program that are available on campus and in the community such as COD Youth Education, STEMCON, and local events.

II-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 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

While College of DuPage has not hosted an Advanced GenCyber Student Camp in previous years, many of the suggestions from the College of DuPage GenCyber 2018 Student Camp Site Visit Report can be applied to the proposed Advanced Student camp. Overall, the 2018 Site Visit report is very positive with a few recommendations to incorporate in future camps, including:

<u>CONCERN</u>	<u>RECOMMENDATION</u>
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 is 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) 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, with state-of-the-art facilities and equipment, as well as innovative curriculum. The Computer and Information 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. This team of experts will develop the camp curriculum and provide instruction at the camp. A variety of subject matter experts from the field will be brought in to enhance the program.

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

Tom Brady, Instructor (Associate Dean, Homeland Security Training Institute, College of DuPage) Mr. Brady holds a MSc. in Integrated Homeland Security Management and 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.

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.

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 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.

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

Student Aide 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 Advanced Student Camp is designed to build off that dedication. The camp's participants come from a dedicated and diverse set of applicants, who are interested in cybersecurity and the First Principles. The 2019 camp will expand upon the success of the 2017 and 2018 GenCyber Student Camps to bring a larger overall impact to 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.