Affordable Materials Grants, Round 19:

Continuous Improvement Grants

(Spring 2021 -Spring 2022)

Proposal Form and Narrative

# Notes

* The proposal form and narrative .docx file is for offline drafting and for our review processes. Submitters must use the online Google Form for proposal submission, including uploading this document.
* The only way to submit the official proposal is through the Google Form. The link to the online application is on the [Round 19 RFP Page](https://www.affordablelearninggeorgia.org/about/rfp_r19).
* The italic text provided below is meant for clarifications and can be deleted.

The Round 18 Kickoff will include an asynchronous training module, required for all team members to complete, followed by the synchronous Kickoff Meeting on March 26, 2021 from 1pm-4pm. At least two team members from each awarded team (unless the award is for one individual) are required to attend the synchronous Kickoff Meeting.

# Applicant and Team Information

*The* ***applicant*** *is the proposed Project Lead for the grant project. The* ***submitter*** *is the person submitting the application (which may be a Grants Officer or Administrator). The submitter will often be the applicant—if so, just leave the submitter blank.*

|  |  |
| --- | --- |
| Requested information | Answer |
| Institution | Kennesaw State University |
| Applicant name | Hossain Shahriar |
| Applicant email  | hshahria@kennesaw.edu |
| Applicant position/title | Associate Professor of Information Technology, Director of Research and Graduate Education, ICWD |
| Submitter name  | Hossain Shahriar |
| Submitter email  | hshahria@kennesaw.edu |
| Submitter position/title | Associate Professor of Information Technology, Director of Research and Graduate Education, ICWD |

Please provide the first/last names and email addresses of all team members within the proposed project. Include the applicant (Project Lead) in this list. Do not include prefixes or suffixes such as Ms., Dr., Ph.D., etc.

|  |  |  |
| --- | --- | --- |
| Team member | Name | Email address |
| Team member 1 | Hossain Shahriar  | hshahria@kennesaw.edu |
| Team member 2 | Meng Han | mhan9@kennesaw.edu |
| Team member 3 | Maria Valero | mvalero2@kennesaw.edu |
| Team member 4 | Liang Zhao | lzhao10@kennesaw.edu |
| Team member 5 | Shirley Tian | xtian2@kennesaw.edu |

If you have any more team members to add, please enter their names and email addresses in the text box below.

|  |
| --- |
| Paweena Somjit; psomjit1@kennesaw.edu Michael Handlin; mhandlin@students.kennesaw.edu |

# Project Information

| Requested information | Answer |
| --- | --- |
| Type of Project | * *Revision of open educational resources (OER) used in existing courses*
* *Creation of ancillaries for existing OER courses*
* *Replacement of current OER in courses with new/better OER*
* ***Other***
 |
| Requested Amount of Funding*$10,000 maximum total award per grant* | *$10,000* |
| Course Titles and Course Numbers | IT 7303 Data Privacy Technologies IT 7313 Physical IT Systems Security IT 7333 Enterprise Cloud and Wireless Security IT 7733 Fundamentals of Enterprise Cloud |
| Final Semester of Project | * *Fall 2021*
* *Spring 2022*
 |
| Currently Existing Resource(s) to be Revised/Ancillaries Created*Please provide a title and web address (URL) to each of the currently existing resources that you are revising, creating new ancillary materials for, or replacing. If replacing, please include a title and web address (URL) to the new OER as well.* | We are creating new materials for the four new courses that are part of MSIT curriculum to start in Fall 2021. Given that they were not prior supported by ALG before to list any URL of prior course materials |

# Project Goals

*In at least one paragraph, describe your project’s goals and what materials will be created or revised.*

The Department of Information Technology at Kennesaw State University (KSU) has taken department-wide efforts to adopt open educational resources (OER) in both undergraduate and graduate courses since 2014. Many thanks to strong support from Affordable Learning Georgia (ALG), all of the courses from MSIT program now has replaced their textbooks with no-cost-to-student OER learning materials. Information technology is an ever-changing field; it is very important to keep our courses updated. The MSIT degree program periodically undergoes curriculum revision every three years. Out of this, we are planning to offer 4 new courses in the direction of cybersecurity and enterprise management starting Fall 2021 as follows:

* IT 7303 - Data Privacy Technologies
* IT 7313 - Physical IT Systems Security
* IT 7333 - Enterprise Cloud and Wireless Security
* IT 7733 - Fundamentals of Enterprise Cloud

As part of our department ALG strategic plan, we propose to create OER materials for these four courses to keep up the MSIT Z-Degree. Our assigned faculty to develop these courses have already identified the preliminary sources based on the learning objectives for developing OER materials. We are striving to make OER resources accessible to all students, as a result, further effort is needed to make developed slides, lectures, test questions compliant with accessibility criteria enforced by Digital Learning Innovation at KSU. The overall goals of our project are listed as follows. The specific plan about each individual course is illustrated in the action plan section.

* Develop new OER materials for courses to be part of MSIT Z Degree
* Ensure all developed OER materials are free from any accessibility issues;
* Develop new OER materials based on course learning outcomes;
* Develop new ancillary material such as assignments, lab material, and test banks;
* Use a department provided layout template to make sure OER material in each course has similar look and feel;
* Ensure all course material comply with the specific accessibility standards defined by ALG;
* Create a course package that can be imported into D2L Brightspace, the course management system used by the University System of Georgia.

# Action Plan

*Describe the tasks needed to complete the project in as much detail as possible. If this application has more than one team member, include the major roles for each person and which tasks this role is assigned. Estimate the amount of time (e.g. number of hours) each task will take. Include plans for open licensing and plans for making your materials accessible. Indicate if you are using other platforms in addition to the repository to host your created materials.*

Our project team is composed of five faculty developers, one instructional designer, and one student assistant. One of the faculty developers, Dr. Hossain Shahriar, assumes the role of the team lead. The detailed project plan is listed as follows.

1. *Project Coordination*. Dr. Hossain Shahriar, who has led several ALG grants from previous rounds, will coordinate the activities in this project to ensure its successful completion. The activities include making a project plan once funded, monitoring project progress, coordinating with university grant office on project budget and expense, facilitating coordination among faculty developers, instructional designer, and student, collecting students’ feedback on the updated OER material and writing semester status report and final report. Dr. Shahriar is estimated to work 30 hours as a project lead role.
2. *Accessibility Compliance*. Ms. Paweena Somjit, an instructional designer at KSU will take a lead role to ensure OER material in the proposed courses comply with the accessibility standards defined by ALG. The faculty developers, Dr. Shahriar, Dr. Han, Dr. Tian, Dr. Valero and Dr. Zhao have completed an Americans with Disabilities Act (ADA) compliance training workshop offered by KSU Digital Learning Innovation center. Ms. Paweena will perform the following activities:
* Research the ALG accessibility requirements specified by ALG (2 hours);
* Conduct accessibility training for faculty developers at the beginning of the project (3 hours);
* Work with faculty developers on accessibility-related issues during the project (25 hours).

The Digital Learning Innovations center of KSU provides manual captioning service for video lectures 15 minutes or less in length. All faculty developers are advised to consider available captioning service when recording their lectures. This will significantly reduce the time faculty or Ms. Paweena spent on accessibility compliance issues. Ms. Paweena is estimated to work 30 hours in this project.

1. *Student Assessment*. Mr. Michael Handlin’s role is to provide feedback on the selected OER material from a student perspective. Mr. Handlin graduated from BS in Computer Science (BSCS) program and currently is enrolled in the MS in Information Technology (MSIT) program at KSU. He has the technical background and experience to evaluate a student. A complete learning module from each proposed course will be given to Mr. Handlin. Mr. Handlin will study the assigned module as a student and provide feedback on the following perspectives:
* Is the OER material user friendly (presentation and structure)?
* Is the content material easy to follow (an appropriate level of difficulty)?
* Is the OER material sufficient for me to complete a quiz/discussion/assignment in this module?

By the estimate, Mr. Handlin will spend 4 hours per course. Total of 20 hours in this project.

1. *Publication of OER material*. All OER material for the proposed courses will be hosted on a public website with a Creative Commons Attribution license. A course package that can be imported into the D2L Brightspace course management system will be available for download for each proposed course.
2. *Action Plan for IT 7303 –Data Privacy Technology*

Faculty developer – Dr. Meng Han. Estimated time working on this course: 50 hours.

Data privacy technologies are technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. The goal of data privacy technology includes increasing control over personal data sent to, and used by, online service providers and merchants. This course will introduce the fundamental concept of data privacy and privacy preserving technologies. In this project, we propose to develop the no coast learning material to enhance the learning experience and update the latest progress in this domain to further benefit our students.

* Module “Laws (GDRP, CCPA, HIPAA, FERPA), regulations and standards for data privacy and digital identity” is going to introduce the major regulation law for data privacy and the technologies relevant with these law policies. The comparison and the trend of the privacy law developed will be introduced. (10 hours are estimated for this task) The faculty developer will create content (slides and video lectures) to explain the concept. The interaction session of the course will also be developed for the students and faculty to establish the discussion on these law establishment along with their behind philosophy. A specific homework will be designed under this model for student further investigate the concepts. Some of the available materials are:
	+ - General data protection regulation: [GDPR official documents](https://gdpr-info.eu/)
		- California Consumer Privacy Act (CCPA): official Act
		- z
		- Health information privacy: [individuals and HIPPA with COVID-19](https://www.hhs.gov/hipaa/index.html)
		- Family educational rights and privacy act: [FERPA official documents](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
* Modules “blockchain technology” will introduce blockchain as a great tool to preserving privacy in multiple different domain and applications. The experiencing of blockchain and the behind infrastructure will be detailed introduced to students. (10 hours are estimated for this task) The faculty developer will create content (slides and video lectures) to explain the concept and tools. Some of the available materials are:
	+ - Security and privacy: [blockchain aspect.](https://arxiv.org/pdf/1903.07602.pdf)
		- Blockchain technology: [security and privacy](https://www.aimsciences.org/article/id/d27803a2-7ce7-46e8-900d-30001fd4785a)
* Modules “privacy issues of collaborative learning” will mainly focuses on the privacy issues and collaborative learning techniques. (10 hours are estimated for this task) The faculty developer will create content (slides and video lectures) to explain the concept and tools. The concepts of federated learning and multiple other techniques will be introduced as well. Some of the available materials are:
	+ - Federated learning: [a step by step implementation.](https://towardsdatascience.com/federated-learning-a-step-by-step-implementation-in-tensorflow-aac568283399)
		- Mitigate AI Bias: [federated Learning as a way](https://www.dataethics4all.org/posts/federated-learning-as-a-way-to-mitigate-ai-bias)
* Modules “managing digital identity” will be developed to introduce the main concept of digital identity management and protection. The student will understand how to use the model and tools to protect and manage the identity. (10 hours are estimated for this task) The faculty developer will create content (slides and video lectures) to explain the concept and tools. The tools of digital identity management will be developed in lab for student to experience. Some of the available materials are:
	+ - The future of identities and how we’ll get there: [identities understanding](https://thycotic.com/company/blog/2020/07/14/digital-identities-the-future-and-how-we-will-get-there/).
		- How to ensure security: [3 types of digital identity](https://searchsecurity.techtarget.com/tip/Using-digital-identity-management-to-gain-and-retain-trust)
* Modules “digital surveillance: methods, tools and privacy regulations” will be designed to introduce the main concept of digital surveillance, and the student will learn how to use the model and tools to understand the regulations. (10 hours are estimated for this task) The faculty developer will create content (slides and video lectures) to explain the concept and tools. Also, the faculty will develop hands-on labs to allow students to further investigate the privacy regulations. Some of the available materials are:
	+ - Global information society watch on data surveillance: [the communication in the digital age.](https://giswatch.org/sites/default/files/digital_surveillance.pdf)
		- How surveillance monitor the world: [the electronic surveillance.](https://www.pinow.com/investigations/electronic-surveillance)

Dr. Han will synthesize the content from those web resources and organize them into OER format. In addition, Dr. Han will record lectures for each module and create ancillary material such as test bank, assignment, and lab. Dr. Meng Han is estimated to spend 25 hours on this task. Also, the faculty developer will work closely with the Department librarian to develop an online Wiki with all the available resources of the course and research papers related to physical security. The student will be able to use this Wiki to find free and open-source materials to develop a team project.

1. *Action Plan for IT 7313 – Physical IT Systems Security*

Faculty developers – (i) Dr. Maria Valero. Estimated time working on this course: 50 hours. (ii) Dr. Hossain Shahriar. Estimated time working on this course: 20 hours.

The current advances in physical devices have led to multiple applications that may be targeted by diverse types of attacks and threats. This course will introduce fundamental security and resilience issues in physical IT systems. Cyber-attacks may impact physical systems and can bypass the traditional cyber defense mechanism. Principles, analyzing the vulnerabilities and threats, attack detection, and defense mechanisms with hands-on tools will be introduced in several IT physical systems including but not limited to IoT, energy, smart health, and autonomous vehicles. This course will be developed with accessible and open-source resources (including device emulators) to allow the student the interaction with physical measurements for preventing physical attacks in current devices. KSU and the Information technology maintain a pool of physical devices (including Raspberry PIs and Arduinos) that will be used for labs with zero cost for students.

* + *Creation of new OER material*. As IT Physical Systems Security is a new course offered by the IT department, the following new materials will be developed during the grant period.
		- Module 1: “Overview of Physical IT Systems,” “Physical platforms and elements,” and “Principles of secure architecture” the content will be focused on understanding the main physical architecture of some devices and perform some physical examples of security vulnerabilities on those devices (10 hours are estimated for this task). In these modules, the faculty developer plans to introduce hands-on labs with Raspberry Pis and Arduinos (already available for student lend) using available open-source resources like:
			* Intro to Raspberry Pi [physical technology](https://tutorials-raspberrypi.com/raspberry-pi-and-arduino-introduction/)
			* Security certificates on [physical devices](https://tutorials-raspberrypi.com/create-raspberry-pi-ssl-certificate-for-free-with-lets-encrypt/)
			* Accessing [remote devices security](https://tutorials-raspberrypi.com/develop-your-own-raspberry-pi-alexa-skill-and-control-pi-remotely/) and [Github leosac](https://github.com/leosac/leosac)
		- Module 2: “Containers and Dockers” and “Containers to secure physical systems” will be designed to introduce the main concept of container and docker to the student and how to use them for security physical system. (10 hours are estimated for this task) The faculty developer will create content (slides and video lectures) to explain the concept and small video tutorials of how to create dockers and containers. Also, the faculty will develop hands-on labs to allow students to interact with the security content of containers in devices. Some of the available materials are:
			* Raspberry Pi docker installation and functionality: [Get Started with Docker and Raspberry pi](https://www.electromaker.io/tutorial/blog/get-started-with-docker-on-the-raspberry-pi)
			* Container security open-source series: [Docker security selinux](https://opensource.com/business/14/7/docker-security-selinux)
		- Module 3: “Security issues in physical systems (sensor, actuators, hardware) – session hijacking, social engineering,” “Emulating a physical system,” “Emulating a physical system, SCADA security” will be designed with open-source emulators that will allow the students to interact with emulated physical systems and communication between them. (15 hours are estimated for this task) The faculty developer will create content (lectures and video tutorials) to teach the basics of emulators for physical systems. Also, hands-on labs will be designed using:
			* The Common Open Research (CORE) Emulator:
			 that is an open-source emulator originally developed US Navy.
			* [SCADA security resources](https://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/)
		- Module 4: “Defense mechanism for physical IT system – Design Secure DMZ, secure firewall, IDS,” “Cloud Integration with physical systems,” and “Secure Cloud Integration with physical systems” will be designed to allow the student to perform interactions between the physical device and the Cloud. (10 hours are estimated for this task). Dr. Hossain Shahriar will create video tutorials, slides, and hands-on labs that allow the student to send data from the physical device to the cloud securely. Some of the available resources are:
			* [Grafana visualization](https://grafana.com/): Open-source and powerful tool to visualize stream data that come from physical devices.
			* HTTPS labs: [MITM proxy](https://mitmproxy.org/)
			* [Secure systems / Firewalls](https://opensource.com/article/19/3/home-lab)
		- Module 5: “Autonomous Vehicle Overview, design of vehicle system” and “Autonomous Vehicle Safety Guidelines, Requirement, CAN BUS introduction” will be designed to allow the student to interact with the main concepts and labs regarding autonomous vehicle safety. Dr. Hossain Shahriar will develop slides, videos, and hands-on materials on these modules. (10 hours are estimated for this task). Some of the content available include
			* [Autonomous vehicles technology](https://www.rand.org/pubs/research_reports/RR443-2.html)
			* [CAN BUS introduction](https://www.youtube.com/watch?v=FqLDpHsxvf8&feature=youtu.be)
		- Module 6: “Smart home sensors. Introduction to Amazon Alexa and Google Home” will be developed to allow the students to interact with emulator scenarios of google home and or amazon Alexa technologies. (15 hours are estimated for this task). The faculty developer will utilize emulators for teaching the security trends on smart home components.
			* [Google Home emulator](https://developers.google.com/assistant/console/simulator)
			* [Amazon Alexa emulator](https://developer.amazon.com/en-US/docs/alexa/devconsole/test-your-skill.html)
	+ Creating video lectures/tutorials for the course. In this project, the faculty developers aim to record one or more video lectures/tutorials for each module to either guide students through the development process or highlight important concepts or information that may be overlooked otherwise. Also, the faculty developer will work closely with the Department librarian to develop an online Wiki with all the available resources of the course and research papers related to physical security. The student will be able to use this Wiki to find free and open-source materials to develop a team project
1. *Action Plan for IT 7333 Enterprise Cloud and Wireless Security*

Faculty developer – Dr. Liang Zhao. Estimated time working on this course: 50 hours.

More businesses than ever are moving sensitive data and shifting mission-critical workloads to the cloud. Organizations are responsible for securing their data and mission-critical applications in the cloud. Wireless networks and devices lack robust security tools—such as firewalls, intrusion prevention systems, content filters, and antivirus and anti-malware detection programs, which are commonly used in wired networks. Thus, they are vulnerable to a variety of attacks designed to gain access to an enterprise network. This course is an advanced study and analysis of the concepts, methodologies and technologies in securing enterprise cloud and wireless networks. Topics include but not limited to wireless network protocols, wireless LAN security tools, cloud computing infrastructure, evolution of cloud, confidentiality and integrity of cloud, and current trends in cloud and wireless security. By the end of this course, a student should be able to explain enterprise cloud and wireless network threats and vulnerabilities along with current security solutions; Describe the differences between wireless security and wired security; Apply security tools to assess and protect enterprise cloud and wireless systems; Conduct research in advanced topics in enterprise cloud systems and wireless networks.

*Creation of new OER material*. As this is a new course expanding MSIT curriculum, Dr. Zhao will develop the course using new accessible and open-source materials, the detailed list of modules are as follows.

* Module 1: The Evolution of Wireless Network
	+ This module introduces wireless network basics. Topics include but not limited to history of wireless networking, OSI model and functionality, and MAC & IP address. Open-source materials such as documentation and websites will be linked in the course. 3 hours are estimated for this task.
	+ [History of wireless networking](http://www.cablefree.net/wireless-technology/history-of-wifi-technology/)
	+ [OSI model and functionality](https://en.wikipedia.org/wiki/OSI_model)
	+ [MAC and IP address](https://searchnetworking.techtarget.com/answer/What-is-the-difference-between-an-IP-address-and-a-physical-address)
* Module 2: Information Security Essentials
	+ This module introduces information security essentials. Topics include but not limited to information security concepts, five pillars of information security, and information security regulatory compliances. 3 hours are estimated for this task.
	+ [Information security concepts](https://en.wikipedia.org/wiki/Information_security)
	+ [Five pillars of information security](https://resourcecenter.infinit-o.com/blog/the-5-pillars-of-information-security-and-how-to-manage-them/)
	+ [Information security compliance](https://www.tcdi.com/information-security-compliance-which-regulations/)
* Module 3: WLAN Overview
	+ This module provides an overview of WLAN. Topics include but not limited to WLAN fundamentals, 802.11 standards, and WLAN topologies and design. 3 hours are estimated for this task.
	+ [WLAN fundamentals](https://en.wikipedia.org/wiki/Wireless_LAN)
	+ [802.11 standards](https://www.networkworld.com/article/3238664/80211x-wi-fi-standards-and-speeds-explained.html)
	+ [WLAN topologies and design](http://student.ing-steen.se/wlan/Chapter_5.pdf)
* Module 4: WLAN Threats & Vulnerabilities
	+ This module discusses WLAN threats & vulnerabilities. Topics include but not limited to types of attackers, overview of vulnerabilities of WLAN, and WEP, WPA and WPA2 vulnerabilities. 3 hours are estimated for this task.
	+ [Types of attackers](https://www.futurelearn.com/info/courses/the-cyber-security-landscape-et/0/steps/60317)
	+ [Overview of WLAN vulnerabilities](https://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf)
	+ [Vulnerabilities of WLAN protocols](https://www.itperfection.com/network-security/wireless-security-protocols-wep-wpa1-wpa2-sae-wsp-wpa3-aes-tkip-network-cybersecurity-cyber/)
* Module 5: WLAN Security
	+ This module covers the security measures for wireless network. Topics include but not limited to architecture for securing wireless network, measures for access control and authentication in WLAN, and data protection in enterprise wireless networks. 3 hours are estimated for this task.
	+ [Secure Wireless Architecture](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch2_2_SPMb.html)
	+ [Measures for access control and authentication](https://www.interlinknetworks.com/whitepapers/WLAN_Access_Control.pdf)
	+ [Data protection in enterprise wireless networks](https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/)
* Module 6: WLAN Security Tools
	+ This module will explore various WLAN security tools. Topics include but not limited to built-in commonly used network utilities tools for Windows and Mac OS, WLAN discovery tools such as NetStumbler, InSSIDer, Kismet and HeatMapper, network protocol analyzing tools such as Aircrack-ng, Wireshark and Airshark, and penetration testing tools such as metasploit and SARA. 3 hours are estimated for this task.
	+ [Network utility tools for Windows](http://techgenix.com/top-11-networking-commands/)
	+ [NetStumbler](http://stumbler.net/)
	+ [Aircrack-ng](https://www.aircrack-ng.org/)
	+ [metasploit](https://metasploit.com/)
* Module 7: Mobile Network Security Threats & Vulnerabilities
	+ This module will cover mobile network security threats and vulnerabilities. Topics include but not limited to Google Android security architecture, Android security challenges, exploitation tools for Android, and BYOD and its security implications. 3 hours are estimated for this task.
	+ [Google Android security architecture](https://source.android.com/security/)
	+ [Android security challenges](https://www.cse.wustl.edu/~jain/cse571-14/ftp/android_security.pdf)
	+ [Exploitation tools for Android](https://geekviews.tech/androrat/)
	+ [BYOD and its security implications](https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating)
* Module 8: Wireless Security Auditing & Risk Analysis
	+ This module will discuss wireless security auditing & risk analysis. Topics include but not limited to concepts and types of security audit, best practices for security audit, tools used for security audit, and wireless security risk analysis framework. 3 hours are estimated for this task.
	+ [Definition of security audit](https://blog.netwrix.com/2020/04/09/it-security-audit/)
	+ [Best practices for security audit](https://internalaudit.wayne.edu/security-practices)
	+ [Wireless security audit tools](https://www.tutorialspoint.com/wireless_security/wireless_security_tools.htm)
	+ [Wireless network risk analysis framework](https://www.diva-portal.org/smash/get/diva2%3A831198/FULLTEXT01.pdf)
* Module 9: Evolution of Cloud
	+ This module will discuss the evolution of cloud. Topics include but not limited to introduction of cloud, overview of evolution of cloud, and cloud service and deployment models. 3 hours are estimated for this task.
	+ [Introduction to cloud](https://www.youtube.com/watch?v=usYySG1nbfI&ab_channel=edureka%21)  (video)
	+ [Evolution of cloud](https://dspace.mit.edu/bitstream/handle/1721.1/100311/932065967-MIT.pdf;sequence=1)
	+ [Cloud service models](https://www.doi.gov/cloud/service)
	+ [Cloud deployment models](https://phoenixnap.com/blog/cloud-deployment-models)
* Module 10: Confidentiality and Integrity of Cloud
	+ This module explores data security in the cloud. Topics include but not limited to cloud data security overview, data privacy in cloud, and protection schemes for cloud data services. The open-source links will be used in this module. 3 hours are estimated for this task.
	+ [Cloud confidentiality and integrity](https://journals.sagepub.com/doi/pdf/10.1155/2014/190903)
	+ [Data privacy in cloud](https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.PDF)
	+ [Protection for cloud data services](https://web.archive.org/web/20160406214320/http%3A/www.4over6.edu.cn/cuiyong/lunwen/Ensuring%20Security%20and%20Privacy%20Preservation%20for%20Cloud%20Data%20Services.pdf)
* Module 11: Cloud Threats & Vulnerabilities
	+ This module discusses threats and vulnerabilities in cloud. Topics include top cloud threats and vulnerabilities, threat analysis and modeling for cloud, and mitigations for cloud vulnerabilities. 3 hours are estimated for this task.
	+ [Threats & vulnerabilities in moving to cloud](https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html)
	+ [Threat modeling for cloud](http://docsdrive.com/pdfs/ansinet/jas/2015/953-967.pdf)
	+ [Mitigating Cloud Vulnerabilities](https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF)
* Module 12: Cloud Security
	+ This module introduces the cloud security basics. Topics include but not limited to cloud deployment models and security, cloud security architecture, and cloud security best practices. Open-source materials such as documentation and websites will be linked in the course. 3 hours are estimated for this task.
	+ [Security issues in cloud deployment models](https://social.technet.microsoft.com/wiki/contents/articles/4509.security-issues-in-cloud-deployment-models.aspx)
	+ [Introduction to cloud security architecture](https://www.infoq.com/articles/cloud-security-architecture-intro/)
	+ [Best practices for cloud security](https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html)

*Creating video tutorials, test banks, quizzes, assignments, projects and discussions for the course*. In this project, the faculty developer will synthesize the content from those web resources and record video lectures for each module to facilitate student learning. In addition, ancillary material such as test bank, quizzes, assignments, projects, and discussions will be developed based on the content in the learning modules. Dr. Liang Zhao is estimated to spend 14 hours on this task.

1. *Action Plan for IT 7733 Fundamentals of Enterprise Cloud*

Faculty developer – Dr. Shirley Tian. Estimated time working on this course: 50 hours.

According to Thomason Reuters (<https://tax.thomsonreuters.com/blog/trends-in-cloud-computing/>), many multinational organizations are going through finance, tax, or IT transformation project to drive efficiency and reduce costs. Amazon AWS is the world’s best comprehensive and broadly adopted cloud platform, offering 165 fully featured services from data center globally. This course will cover the fundamental ideas behind enterprise cloud, the evolution of the paradigm, its applicability; benefits, as well as current and future challenges; The basic ideas and principles in enterprise cloud; cloud management techniques and enterprise cloud deployment considerations; Cloud storage technologies and relevant distributed file systems, NoSQL databases and object storage. The course also covers the hands-on labs to practice on the cloud platform. Dr. Tian is the Amazon AWS accredit educator and KSU is the AWS accredit institution. Students can use the Amazon AWS materials and labs free of charge. By the end of this course, a student should be able to define and explain enterprise cloud with a focus on the Cloud, its architecture, and its global infrastructure; Describe and use security and compliance measures of enterprise cloud; Utilize IT cost and control concepts, e.g., total cost of ownership, and tools for comparing on-premises IT, cloud IT and hybrid IT with a focus on the cloud scaling, monitoring, costing, and pricing tools; Explain and arrange the fundamental components of enterprise cloud, including networking and content delivery, compute, storage, and databases, practice in labs. Video lectures will also be created for each module. Since this course is a brand-new course, the detailed list of modules and improvements are as follows.

* Module 1: Course overview and background of cloud
	+ All the instructions, along with screenshots and other materials will be used in the module. Due to the nature of the course, most of the content in the course is custom instructions developed by the faculty developer. External resources such as the documentation websites will be linked in the course as supplemental readings where appropriate. 3 hours are estimated for this task.
	+ Introduction to cloud computing
	+ [The background of cloud computing](http://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/BackgroundofCloudComputing.aspx)
	+ [Amazon AWS introduction](https://aws.amazon.com/getting-started/)
* Module 2: Cloud concepts
	+ This module introduces the cloud concepts. Two major cloud platforms in the market will be introduced. The advantages of the cloud will be introduced as well. The open-source links will be used in this module. 3 hours are estimated for this task.
* [AWS cloud concepts](https://aws.amazon.com/getting-started/fundamentals-core-concepts/?e=gs2020&p=gsrc)
* [Benefits of cloud computing](https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/)
* [Advantages and disadvantages of cloud computing](https://www.guru99.com/advantages-disadvantages-cloud-computing.html)
* Module 3: Cloud economics and billing
	+ This module introduces the fundamentals of pricing, total cost of ownership, and billing and cost management. 3 hours are estimated for this task.
* [Cloud economics in Azure](https://azure.microsoft.com/en-us/overview/cloud-economics/)
* [Cloud economics in AWS](https://aws.amazon.com/economics/)
* [Understanding the Total Cost of Ownership](https://cdn2.hubspot.net/hub/49708/file-14401780-pdf/docs/whitepaper_%20moving_to_the_cloud-_understanding_the_total_cost_of_ownership_pdf)
* [The real cost of cloud computing](https://cloud.vmware.com/community/2019/01/17/real-cost-cloud-computing/)
* [Azure Total cost ownership calculator](../Total%20Cost%20of%20Ownership%20%28TCO%29%20Calculator)
* [Video: Total cost of ownership of cloud](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjK8Ojw2fnuAhUNm-AKHWS3BUo4ChC3AjAAegQIChAD&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DQlRqTP2bcXw&usg=AOvVaw0ewOZ4_ot7KiKUgtK2Z2ag)
* Module 4: Cloud Global Infrastructure
	+ Cloud global infrastructure will be introduced. Cloud service categories of services (computing, storage, network) will be covered as well. 3 hours are estimated for this task.
	+ [Azure global infrastructure](https://azure.microsoft.com/en-us/global-infrastructure/)
	+ [AWS global infrastructure](https://aws.amazon.com/about-aws/global-infrastructure/)
* Module 5: Cloud security
	+ Cloud security will cover the shared responsibility model, securing accounts, securing data, and ensure compliance. AWS Identity and Access Management (IAM) will be introduced. 3 hours are estimated for this task.
	+ [AWS Cloud Security](https://aws.amazon.com/security/)
	+ [What is different about cloud security](https://www.redhat.com/en/topics/security/cloud-security)
	+ [Video: What is cloud security](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=video&cd=&cad=rja&uact=8&ved=2ahUKEwjvgKXk3vnuAhWGHc0KHUFfAscQtwIwAHoECAMQAw&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DjI8IKpjiCSM&usg=AOvVaw20-uwgggQ0NsVrRQ2tfcfT)
* Module 6: Networking
	+ Networking management in cloud. This module will use Amazon AWS as an example to introduce the network basis, VPC networking and security. 3 hours are estimated for this task.
	+ [Video: cloud computing basics for beginners](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=video&cd=&cad=rja&uact=8&ved=2ahUKEwit_aPZ3_nuAhWXZM0KHZTbCLgQtwIwA3oECAYQAw&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DC8Z452C18JE&usg=AOvVaw1oPMtv_wSJz5OOaLDcGwLt)
	+ [Video: Cloud computing basics of networking](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjpvOWJ4PnuAhXtnuAKHeLNCLA4ChC3AjAAegQIChAD&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DzuJHiJYt9Q0&usg=AOvVaw1C5FX7XluWs_tpC9JLaWi-)
	+ [Amazon VPC](https://aws.amazon.com/vpc/?vpc-blogs.sort-by=item.additionalFields.createdDate&vpc-blogs.sort-order=desc)
* Module 7: Content delivery
* Cloud content delivery network will be covered in this module. A content delivery network (CDN) is a globally distributed system of caching servers. A CDN caches copies of commonly requested files (static content, such as Hypertext Markup Language, or HTML; Cascading Style Sheets, or CSS; JavaScript; and image files) that are hosted on the application origin server. The CDN delivers a local copy of the requested content from a cache edge or Point of Presence that provides the fastest delivery to the requester. 3 hours are estimated for this task.
	+ [Amazon CloudFront](https://aws.amazon.com/cloudfront/)
	+ [What is a CDN? How do CDNs work?](https://www.cloudflare.com/learning/cdn/what-is-a-cdn/)
* Module 8: Compute
	+ This module will provide an overview of different AWS compute services in the cloud. Compare and choose the best practice for the organization. This module will use the Amazon AWS as the example. 3 hours are estimated for this task.
	+ [Amazon EC2: Secure and resizable compute capacity to support virtually any workload](https://aws.amazon.com/ec2/?ec2-whats-new.sort-by=item.additionalFields.postDateTime&ec2-whats-new.sort-order=desc)
	+ Amazon EC2 hands-on lab will be included.
* Module 9: Storage and Databases
	+ Cloud storage is typically more reliable, scalable, and secure than traditional on-premises storage system. Cloud storage is a critical components of cloud computing because it holds the information that applications use. Big data analytics, data warehouses, the Internet of Things (IoT), databases, and backup and archive applications all rely on some form of data storage architecture. This module will use Amazon AWS as the example to discuss different types of storage in the cloud computing. 3 hours are estimated for this task.
	+ [Cloud Storage](https://aws.amazon.com/what-is-cloud-storage/)
	+ [Benefits of cloud storage and types of storage](https://aws.amazon.com/what-is-cloud-storage/)
	+ [Five ways to use cloud storage](https://aws.amazon.com/what-is-cloud-storage/)
* Module 10: Cloud architecture
	+ This module will include AWS well-architected framework, reliability and high availability, AWS Trusted Advisor. Students will be challenged to review an architecture and evaluate it against the AWS Well-Architected Framework design principles. 3 hours are estimated for this task.
	+ [The 3 layers that define cloud computing](https://blog.thriveon.net/cloud-computing)
	+ [Reference: AWS Architecture Center](https://aws.amazon.com/architecture/)
* Module 11: Automatic scaling
	+ This module will introduce Amazon Elastic Compute Cloud, EC2 Auto Scaling launches and releases servers in respond to the workload changes. 3 hours are estimated for this task.
	+ [AWS Auto Scaling](https://aws.amazon.com/autoscaling/)
* Module 12: Automatic monitoring
	+ Amazon CloudWatch is a monitoring and observability service that is built for DevOps engineers, developers, site reliability engineers and IT managers. 3 hours are estimated for this task.
	+ [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/)
* Module 13: Cloud adoption case study
	+ 3 hours are estimated for this task.
	+ [10 important cloud migration case studies you need to know](https://distillery.com/blog/cloud-migration-case-studies/)
	+ [AWS Case study](https://aws.amazon.com/solutions/case-studies/?customer-references-cards.sort-by=item.additionalFields.publishedDate&customer-references-cards.sort-order=desc)
	+ [Deloitte cloud case study](https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-deloitte-onsite-workforce-client-story.pdf)

*Creating video tutorials for the course*. Outside of the online resources that are presented as URLs in the course, the learning content in the current course is entirely text-based. In this project, the faculty developer aims to record one or more video lectures/tutorials for each module to either guide students through the development process or highlight important concepts or information that may be overlooked otherwise. 8 hours are estimated for this task.

 *Creating test banks, quizzes, assignments and labs, and discussions.* According to the learning outcomes for the courses and each module, the tests, quizzes, assignments, labs, and discussions will be based on the learning materials that covered in the modules. And external readings will be introduced for discussion purpose. Lab contents will be offered by Amazon AWS. 6 hours are estimated for this task.

# Timeline

*Provide a project timeline aligned with the action plan above. Include major milestones and deadlines, keeping in mind your selected Final Semester.*

In the section, we first describe the overall project timeline. The timeline for each proposed course is listed separately.

1. *Overall Project Timeline – Responsible personal: Dr. Hossain Shahriar*
	1. *4/1/2021*. Complete accessibility training and review of existing OER material.
	2. *8/15/2021*. a) Complete the development of accessibility compliant OER material; b) Complete the project progress report.
	3. *12/30/2021*. a). Complete the development of accessibility compliant OER ancillary material such as quizzes, test banks, assignment and/or labs; b) Complete student review of the OER material; c). Develop an online survey instrument for collecting students’ feedback after courses are taught using updated OER material; d) Complete the project progress report.
	4. *5/15/2022*. a). Complete course offerings with updated OER material. b). Complete the course survey on updated OER material; c). Publish the updated OER material in a public website and create a course package that can be imported into D2L. d). Compile and submit the final project report.
2. *Timeline for IT 7303– Data Privacy Technology - Responsible personal: Dr. Meng Han*
3. *4/1/2021*. Complete accessibility training. Complete module 1 – 9.
4. *8/15/2021*. a). Complete the development of accessibility compliant OER material b). Complete expanding modules 10 – 13. c). Complete complying all OER materials and accessibility to ALG standards.
5. *12/30/2021*. a). Complete the development of accessibility compliant OER ancillary material such as quizzes, test banks, and assignment; b). Conduct student review of the OER material; c) Improve the course materials based on the received feedback.
6. *5/15/2022*. a). Complete course offerings with updated OER material. b). Collect students’ feedback on the course; c). Publish the updated OER material in a public website and create a course package that can be imported into D2L.
7. *Timeline for IT 7313 – Physical IT Systems Security: Dr. Maria Valero*
8. *4/1/2021*. a). Complete/review accessibility training and requirements. b). Review the content of OER material in existing modules. c). check for accessibility issues of existing modules.
9. *8/15/2021*. Complete the development of accessibility compliant OER material for six new learning modules. The existing OER material will be updated and comply with accessibility standards set by ALG.
10. *12/30/2021*. a). Complete the development of accessibility compliant OER ancillary material such as quizzes, tests, and labs; b) Perform the learning module student review by Michael Handlin. Improve the module and other modules based on the feedback received from Michael.
11. *5/15/2021*. a). Complete the first-time course offering with updated OER material. b). Collect students’ feedback on updated OER material; c). Publish all the OER material to the website and the D2L course management system.
12. *Timeline for IT 7333 – Enterprise Cloud and Wireless Security – Responsible personal: Dr. Liang Zhao*
	1. *4/1/2021*. Complete/review accessibility training and requirements. Review the existing course, collect necessary materials and resources, and prepare a detailed task list for the update/redevelopment.
	2. *8/15/2021*. a). Complete updating the instructions in the course to the current release of the MEAN stack. Learning materials for new topics such as DevOps will also be developed.
	3. *12/30/2021*. a). Complete the redevelopment of accessibility compliant course materials in HTML format, along with the video lectures.
	4. *5/15/2022*. a). Complete course offerings with updated OER material. b). Collect students’ feedback on the course; c). Publish the updated OER material in a public website and create a course package that can be imported into D2L.
13. *Timeline for IT 7733 - Fundamentals of Enterprise Cloud - Responsible personal: Dr. Shirley Tian*
14. *4/1/2021*. a). Complete/review accessibility training and requirements b). Collecting necessary materials and creating the course plan. C) Syllabus development
15. *8/15/2021*. Complete the development of accessibility compliant OER material for learning modules 1-6.
16. *12/30/2021*. a). Complete the development of accessibility compliant OER ancillary material such as quizzes, test banks, and labs for modules 1-6; b) Send one learning module to Michael Handlin for student review. Revise the module and other modules based on the feedbacks received. C) Continue to develop modules 7-13.
17. *5/15/2022*. a). Complete course offering with update OER material. b). Collect students’ feedback on updated OER material; c). Host the OER material in a publicly available website and create a course package that can be imported into D2L.

# Budget

*Please enter your project’s budget below. Include personnel and projected expenses, keeping in mind that this grant funds the estimated time in your Action Plan. The maximum amounts for the award are as follows:*

* *$2,000 maximum per team member for salary, course release, travel, etc.*
* *Additional project expenses allowed, but must be adequately justified in this section*
* *$10,000 maximum total award per grant*

The budget of this proposal is listed as follows.

* Dr. Hossain Shahriar, project lead, co-developer for IT 7313, $1600 for summer salary.
* Dr. Meng Han, developer and instructor of record for IT 7303, $1800 for summer salary.
* Dr. Maria Valero, co-developer and instructor of record for IT 7313, $1800 for summer salary.
* Dr. Liang Zhao, developer and instructor of record for IT 7333, $1800 for summer salary.
* Dr. Shirley Tian, developer and instructor of record for IT 7733, $1800 for summer salary.
* Paweena Somjit, instructional designer, $900 for summer salary.
* Michael Handlin, student reviewer, $300.

# Creative Commons Terms

*I understand that any new materials or revisions created with Affordable Learning Georgia funding will, by default, be made available to the public under a Creative Commons Attribution License (CC-BY), with exceptions for modifications of pre-existing resources with a more restrictive license.*

# Accessibility Terms

*I understand that any new materials or revisions created with Affordable Learning Georgia funding must be developed in compliance with the specific accessibility standards defined in the* [*Request for Proposals*](https://www.affordablelearninggeorgia.org/about/rfp_r18)*.*

# Letter of Support

*The Department Chair from the corresponding project, or the Department Chair’s direct report such as the Dean or Provost, must provide a signed Letter of Support for the project. This letter should acknowledge the following:*

* *The department will provide support for fund disbursement in correspondence with the Grants/Business Office.*
* *The department approves of the work on the proposal by the applicant(s).*
* *The department acknowledges the sustainability of these affordable resources after the grant work is complete.*

*In the case of multi-institutional affiliations, all participants’ institutions must provide a letter of support.*

*Please provide the name and title of the department chair (or other administrator) who provided you with the Letter of Support.*

|  |
| --- |
| *Dr. Rebecca Rutherfoord, Professor of IT, Chair of Department of Information Technology* |

# Grants or Business Office Letter of Acknowledgment

*Institutional Grants/Business Offices will be responsible for fund disbursement, often in correspondence with the Department Chair, including expense and travel reimbursement. Applicants will need to provide a short Letter of Acknowledgment stating that the Grants/Business Office knows about the applicant’s intent to apply for an Affordable Materials Grant. Either the Department Chair or the Project Lead can work with the Grants/Business Office to get this signed letter.*

*In the case of multi-institutional affiliations, all participants’ institutions must provide a letter of acknowledgment.*

*Please provide the name and title of the grants or business office representative who provided you with the Letter of Acknowledgment.*

|  |
| --- |
| Kimberley Hunt, Grants and Contract Manager Office of Research, Kennesaw State University |