Cover Sheet: Request 15274

CIS 4xxx Enterprise Security

Info

Process	Course|New|Ugrad/Pro
Status	Pending at PV - University Curriculum Committee (UCC)
Submitter	Cheryl Resch cheryl.resch@ufl.edu
Created	9/17/2020 1:39:05 PM
Updated	11/6/2020 9:18:01 PM
Description of request	Enterprise Security has been offered as a special topics course. It would be appropriate to offer this course regularly and to offer it as part of the Computer Security track in the CS degree. As such, I'm requesting a regular course number for this course.

Actions

Step	Status	Group	User	Comment	Updated
Department	Approved	ENG - Computer and Information Science and Engineering 19140000	Christina Gardner-McCune		9/25/2020
No document changes					
College	Approved	ENG - College of Engineering	Heidi Dublin	Approved by Curriculum Committee and Faculty Council	10/9/2020
No document changes					
University Curriculum Committee	Pending	PV - University Curriculum Committee (UCC)			10/9/2020
No document changes					
Statewide Course Numbering System					
No document changes					
Office of the Registrar					
No document changes					
Student Academic Support System					
No document changes					
Catalog					
No document changes					
College Notified					
No document changes					

Course|New for request 15274

Info

Request: CIS 4xxx Enterprise Security
Description of request: Enterprise Security has been offered as a special topics course. It would be appropriate to offer this course regularly and to offer it as part of the Computer Security track in the CS degree. As such, I'm requesting a regular course number for this course.
Submitter: Cheryl Resch cheryl.resch@ufl.edu
Created: 11/6/2020 9:17:00 PM
Form version: 5

Responses

Recommended Prefix
Enter the three letter code indicating placement of course within the discipline (e.g., POS, ATR, ENC). Note that for new course proposals, the State Common Numbering System (SCNS) may assign a different prefix.

> Response:
> CIS

Course Level
Select the one digit code preceding the course number that indicates the course level at which the course is taught (e.g., 1=freshman, 2=sophomore, etc.).

> Response:
> 4

Course Number
Enter the three digit code indicating the specific content of the course based on the SCNS taxonomy and course equivalency profiles. For new course requests, this may be XXX until SCNS assigns an appropriate number.

> Response:
> XXX

Category of Instruction
Indicate whether the course is introductory, intermediate or advanced. Introductory courses are those that require no prerequisites and are general in nature. Intermediate courses require some prior preparation in a related area. Advanced courses require specific competencies or knowledge relevant to the topic prior to enrollment.

> Response:
> Intermediate

• 1000 level = Introductory undergraduate
• 2000 level = Introductory undergraduate
• 3000 level = Intermediate undergraduate
• 4000 level = Advanced undergraduate
• 5000 level = Introductory graduate
• 6000 level = Intermediate graduate
• 7000 level = Advanced graduate
• 4000/5000= Joint undergraduate/graduate
• 4000/6000= Joint undergraduate/graduate

*Joint undergraduate/graduate courses must be approved by the UCC and the Graduate Council)

Lab Code

Enter the lab code to indicate whether the course is lecture only (None), lab only (L), or a combined lecture and lab (C).

    Response:
    None

Course Title

*Enter the title of the course as it should appear in the Academic Catalog. There is a 100 character limit for course titles. *

    Response:
    Enterprise Security

Transcript Title

Enter the title that will appear in the transcript and the schedule of courses. Note that this must be limited to 30 characters (including spaces and punctuation).

    Response:
    Enterprise Security

Degree Type

Select the type of degree program for which this course is intended.

    Response:
    Baccalaureate

Delivery Method(s)

Indicate all platforms through which the course is currently planned to be delivered.

    Response:
    On-Campus

Co-Listing

Will this course be jointly taught to undergraduate, graduate, and/or professional students?

    Response:
    No

Effective Term

Select the requested term that the course will first be offered. Selecting "Earliest" will allow the course to be active in the earliest term after SCNS approval. If a specific term and year are selected, this should reflect the department's best projection. Courses cannot be implemented retroactively, and therefore the actual effective

term cannot be prior to SCNS approval, which must be obtained prior to the first day of classes for the effective term. SCNS approval typically requires 2 to 6 weeks after approval of the course at UF.

Response:
Spring

Effective Year
Select the requested year that the course will first be offered. See preceding item for further information.

Response:
2021

Rotating Topic?
Select "Yes" if the course can have rotating (varying) topics. These course titles can vary by topic in the Schedule of Courses.

Response:
No

Repeatable Credit?
Select "Yes" if the course may be repeated for credit. If the course will also have rotating topics, be sure to indicate this in the question above.

Response:
No

Amount of Credit
Select the number of credits awarded to the student upon successful completion, or select "Variable" if the course will be offered with variable credit and then indicate the minimum and maximum credits per section. Note that credit hours are regulated by Rule 6A-10.033, FAC. If you select "Variable" for the amount of credit, additional fields will appear in which to indicate the minimum and maximum number of total credits.

Response:
3

S/U Only?
Select "Yes" if all students should be graded as S/U in the course. Note that each course must be entered into the UF curriculum inventory as either letter-graded or S/U. A course may not have both options. However, letter-graded courses allow students to take the course S/U with instructor permission.

Response:
No

Contact Type
Select the best option to describe course contact type. This selection determines whether base hours or headcount hours will be used to determine the total contact hours per credit hour. Note that the headcount hour options are for courses that involve contact between the student and the professor on an individual basis.

Response:
Regularly Scheduled

• Regularly Scheduled [base hr]
• Thesis/Dissertation Supervision [1.0 headcount hr]
• Directed Individual Studies [0.5 headcount hr]
• Supervision of Student Interns [0.8 headcount hr]
• Supervision of Teaching/Research [0.5 headcount hr]
• Supervision of Cooperative Education [0.8 headcount hr]

Contact the Office of Institutional Planning and Research (352-392-0456) with questions regarding contact type.

Weekly Contact Hours
Indicate the number of hours instructors will have contact with students each week on average throughout the duration of the course.

Response:
3

Course Description
Provide a brief narrative description of the course content. This description will be published in the Academic Catalog and is limited to 500 characters or less. See course description guidelines.

Response:
Provides an introduction to the real-world aspects of defending an enterprise network. Students will gain hands-on experience performing system security tasks and handling incidents. The class begins with a basic introduction to enterprise cybersecurity, the attack sequence, and managing cybersecurity. Then lecture, homework and lab activities cover the center for internet security's twenty essential security controls.

Prerequisites
Indicate all requirements that must be satisfied prior to enrollment in the course. Prerequisites will be automatically checked for each student attempting to register for the course. The prerequisite will be published in the Academic Catalog and must be formulated so that it can be enforced in the registration system. Please note that upper division courses (i.e., intermediate or advanced level of instruction) must have proper prerequisites to target the appropriate audience for the course.
Courses level 3000 and above must have a prerequisite.
Please verify that any prerequisite courses listed are active courses.

Response:
COP3530

Completing Prerequisites on UCC forms:

• Use "&" and "or" to conjoin multiple requirements; do not used commas, semicolons, etc.
• Use parentheses to specify groupings in multiple requirements.
• Specifying a course prerequisite (without specifying a grade) assumes the required passing grade is D-. In order to specify a different grade, include the grade in parentheses immediately after the course number. For example, "MAC 2311(B)" indicates that students are required to obtain a grade of B in Calculus I. MAC2311 by itself would only require a grade of D-.
• Specify all majors or minors included (if all majors in a college are acceptable the college code is sufficient).
• "Permission of department" is always an option so it should not be included in any prerequisite or co-requisite.
• If the course prerequisite should list a specific major and/or minor, please provide the plan code for that major/minor (e.g., undergraduate Chemistry major = CHY_BS, undergraduate Disabilities in Society minor =

DIS_UMN)

Example: A grade of C in HSC 3502, passing grades in HSC 3057 or HSC 4558, and undergraduate PBH student should be written as follows: HSC 3502(C) & (HSC 3057 or HSC 4558) & UGPBH
* *

Co-requisites
Indicate all requirements that must be taken concurrently with the course. Co-requisites are not checked by the registration system. If there are none please enter N/A.

Response:
N/A

Rationale and Placement in Curriculum
Explain the rationale for offering the course and its place in the curriculum.

Response:
Provides students with the knowledge necessary to define and implement a security program for the protection of an organizations systems and data. It provides hands-on experience in securing networks and responding to cyber security threats. This fits in with cybersecurity elective courses offered in the CISE department.

Course Objectives
Describe the core knowledge and skills that student should derive from the course. The objectives should be both observable and measurable.

Response:
By the end of the semester, students should be able to
- Identify and think critically about weaknesses in an enterprise network
- Assess risk and prioritize problem areas
- Identify controls to mitigate risk

Course Textbook(s) and/or Other Assigned Reading
*Enter the title, author(s) and publication date of textbooks and/or readings that will be assigned. Please provide specific examples to evaluate the course and identify required textbooks. *

Response:
Verizon Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir

Center for Internet Security Top 20 Security Controls

NIST Special Publication 800-30 Guide to Conducting Risk Assessments

Weekly Schedule of Topics
Provide a projected weekly schedule of topics. This should have sufficient detail to evaluate how the course would meet current curricular needs and the extent to which it overlaps with existing courses at UF.

Response:
Week / Topics / 'NICE Challenge' Lab / Assignment

1 / Defining the cybersecurity challenge, Enterprise security frameworks / none / none
2 / Risk analysis / 'Radical Risk Reduction' / HW1 Risk analysis
3 / Cybersecurity attack sequence, Security policies / 'Malicious malware' / HW2 Research an attack
4 / Inventory and control of hardware and software / 'Assuring accurate asset inventories' / Discussion 1 - hardware/software inventory products
5 / Continuous vulnerability management / 'Vulnerability scan complete, begin system hardening' / Discussion 2 - vulnerability management products
6 / Access control / 'Secure roots: domain organization and access controls'/HW3 Access control
7 / Secure configurations / 'STIG Solutions'
8 / Auditing / 'Legitimate Logging Logistics'
9 / Email and web browser protections / 'Malicious mail management' / Discussion 3 - email and web browser management products
10 / Boundary defense / 'Firewall update: tables for two' / HW4 - Firewalls
11 / Data protection and recovery / 'Data backup and recovery, definitely worth testing' / Discussion 4 - Data backup and recovery products
12 / Security awareness and training / 'Dangerous drives' / Discussion 5 - Security awareness and training
13 / Account monitoring and control / 'Networking anomalies: Policy Implementation'
14 / Incident Handling / 'Malware aftermath clean up'
15 / Penetration tests and read team exercises / 'Penetration Testing: Bringing passwords up to snuff' / Paper

Grading Scheme

List the types of assessments, assignments and other activities that will be used to determine the course grade, and the percentage contribution from each. This list should have sufficient detail to evaluate the course rigor and grade integrity. Include details about the grading rubric and percentage breakdowns for determining grades. If participation and/or attendance are part of the students grade, please provide a rubric or details regarding how those items will be assessed.

Response:

Assignment	Percentage of Final Grade
Labs (14, 1 drop)	50%
Homeworks 4	15%
Discussions 5	15%
Paper	20%

Labs:
Challenge activities from https://nice-challenge.com/. Cooperation and mutual support during the labs is allowed and encouraged.

Discussions:
Discussions are conducted through the Canvas Discussion link. Discussions are assigned on Tuesdays and due on the following Monday. This will entail researching and describing an enterprise security tool for a specific need (e.g. vulnerability scanner).
Rubric
On time post, 3-4 sentences describing tool, features and strengths of tool 10 points
On time post, vague or brief (2 sentences or less) description of tool.

Homeworks:
Homeworks consist of problem solving and will be turned in on Canvas. Per University Honesty Policy, please do your own work.

Paper:
Groups of 2 or 3 will complete a security design for an enterprise of their choice. The paper must include

Asset Identification 20 points
Data assets of the enterprise described. Confidentiality, integrity and availability needs described.

Risk Analysis   20 points
Threat agents for all assets. Possible actions and likelihood for all threat agent/asset pairs. Well thought out and complete listing of threat/action/likelihood/consequence.
User Groups and Access Control 10 points
Types of users described, e.g. who are trusted users, what data can they access.

Controls 20 points
Identify controls for each risk. A framework for the suite of controls, e.g. CIS Top 20, is identified.
Writing and Quality 20 points
Produce a quality product with correct grammar, free of typos, and formatted. Put effort and creativity into the product.
Enterprise 5 points
Introduce the enterprise. What is their product or industry. What most important to this enterprise?

References   5 points
Include references, e.g where you got information on what the threat actors and actions are.

Instructor(s)
Enter the name of the planned instructor or instructors, or "to be determined" if instructors are not yet identified.

Response:
Cheryl Resch

Attendance & Make-up
Please confirm that you have read and understand the University of Florida Attendance policy.
A required statement statement related to class attendance, make-up exams and other work will be included in the syllabus and adhered to in the course. Courses may not have any policies which conflict with the University of Florida policy. The following statement may be used directly in the syllabus.

• Requirements for class attendance and make-up exams, assignments, and other work in this course are consistent with university policies that can be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

Response:
Yes

Accomodations
Please confirm that you have read and understand the University of Florida Accommodations policy.
A statement related to accommodations for students with disabilities will be included in the syllabus and adhered to in the course. The following statement may be used directly in the syllabus:

• Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, www.dso.ufl.edu/drc/) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Response:
Yes

UF Grading Policies for assigning Grade Points
Please confirm that you have read and understand the University of Florida Grading policies.
Information on current UF grading policies for assigning grade points is require to be included in the course syllabus. The following link may be used directly in the syllabus:

• *https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx*

    Response:
    Yes

Course Evaluation Policy
Course Evaluation Policy
Please confirm that you have read and understand the University of Florida Course Evaluation Policy.
A statement related to course evaluations will be included in the syllabus. The following statement may be used directly in the syllabus:

• *Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/public-results/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.*

* *

    Response:
    Yes

Enterprise Security
CIS 4XXX   Section 1234
Class Periods: Tu 3-350 Period 8 / Th 3-455 Period 8,9
Location: Classroom location
Academic Term: Sprint 2021

Instructor:
Cheryl Resch
Cheryl.resch@ufl.edu
Office Hours: M 4pm, Tu 4pm

Course Description
Provides an introduction to the real-world aspects of defending an enterprise network. Students will gain hands-on experience performing system security tasks and handling incidents. The class begins with a basic introduction to enterprise cybersecurity, the attack sequence, and managing cybersecurity. Then lecture, homework and lab activities cover the center for internet security's twenty essential security controls.

Course Pre-Requisites
CDA 3101

Course Objectives
By the end of the semester, students should be able to
- Identify and think critically about weaknesses in an enterprise network
- Assess risk and prioritize problem areas
- Identify controls to mitigate risk

Materials and Supply Fees
none

Relation to Program Outcomes (ABET):

Outcome	Coverage*
1. An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics	Medium
2. An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors	Medium
3. An ability to communicate effectively with a range of audiences	High
4. An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts	
5. An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives	

6. An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions		
7. An ability to acquire and apply new knowledge as needed, using appropriate learning strategies	Medium	

*Coverage is given as high, medium, or low. An empty box indicates that this outcome is not covered or assessed in the course.

Required Textbooks and Software
None

Recommended Materials
None

Course Schedule
Week / Topics / 'NICE Challenge' Lab / Assignment

1 / Defining the cybersecurity challenge, Enterprise security frameworks
2 / Risk analysis / 'Radical Risk Reduction' / HW1 Risk analysis
3 / Cybersecurity attack sequence, Security policies / 'Malicious malware' / HW2 Research an attack
4 / Inventory and control of hardware and software / 'Assuring accurate asset inventories' / Discussion 1 - hardware/software inventory products
5 / Continuous vulnerability management / 'Vulnerability scan complete, begin system hardening' / Discussion 2 - vulnerability management products
6 / Access control / 'Secure roots: domain organization and access controls'/HW3 Access control
7 / Secure configurations / 'STIG Solutions'
8 / Auditing / 'Legitimate Logging Logistics'
9 / Email and web browser protections / 'Malicious mail management' / Discussion 3 - email and web browser management products
10 / Boundary defense / 'Firewall update: tables for two' / HW4 - Firewalls
11 / Data protection and recovery / 'Data backup and recovery, definitely worth testing' / Discussion 4 - Data backup and recovery products
12 / Security awareness and training / 'Dangerous drives' / Discussion 5 - Security awareness and training
13 / Account monitoring and control / 'Networking anomalies: Policy Implementation'
14 / Incident Handling / 'Malware aftermath clean up'
15 / Penetration tests and read team exercises / 'Penetration Testing: Bringing passwords up to snuff' / Paper

We will have face-to-face instructional sessions to accomplish the student learning objectives of this course. In response to COVID-19, the following policies and requirements are in place to maintain your learning environment and to enhance the safety of our in-classroom interactions.

- You are required to wear approved face coverings at all times during class and within buildings. Following and enforcing these policies and requirements are all of our responsibility. Failure to do so will lead to a report to the Office of Student Conduct and Conflict Resolution.

- This course has been assigned a physical classroom with enough capacity to maintain physical distancing (6 feet between individuals) requirements. Please utilize designated seats and maintain appropriate spacing between students. Please do not move desks or stations.

- Sanitizing supplies are available in the classroom if you wish to wipe down your desks prior to sitting down and at the end of the class.

- Follow your instructor's guidance on how to enter and exit the classroom. Practice physical distancing to the extent possible when entering and exiting the classroom.

- If you are experiencing COVID-19 symptoms (Click here for guidance from the CDC on symptoms of coronavirus), please use the UF Health screening system and follow the instructions on whether you are able to attend class. Click here for UF Health guidance on what to do if you have been exposed to or are experiencing Covid-19 symptoms.
- Course materials will be provided to you with an excused absence, and you will be given a reasonable amount of time to make up work. Find more information in the university attendance policies.

Attendance Policy, Class Expectations, and Make-Up Policy
Class attendance on Thursdays for NICE challenges in person or via Zoom is required.

Homeworks, discussions, and the paper must be submitted on time unless there is a university approved excuse. Late assignments will receive no credit.
Excused absences must be in compliance with university policies in the Graduate Catalog (http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance) and require appropriate documentation.

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Labs (14, 1 drop)	100 each	50%
Homeworks (4)	40 each	15%
Discussions (5)	10 each	15%
Paper	100	20%
		100%

Labs
Labs are done on Thursdays during the class period via https://nice-challenge.com/. Each student will have access to a virtual environment where they will carry out tasks as specified in the lab. Students will document how they accomplished each tasks. Collaborating with classmates is welcomed and encouraged. Grading is based on completing and documenting the tasks.

Homeworks
Homeworks consist of problems and short answer questions. They are assigned on Tuesdays and due on the following Monday and may not be turned in late.

Discussions

Discussions are conducted through the Canvas Discussion link. Discussions are assigned on Tuesdays and due on the following Monday. This will entail researching and describing an enterprise security tool for a specific need (e.g. vulnerability scanner).

Rubric

On time post, 3-4 sentences describing tool, features and strengths of tool 10 points

On time post, vague or brief (2 sentences or less) description of tool.

Paper

The paper is due on the last day of the semester and may not be turned in late.

Choose an enterprise. Examples are a university, a company, a county government, an office. Design security for this enterprise.

The paper must include:

Title

Introduction - Describe the enterprise. What industry sector is it in? How large is the enterprise? Brief description of operations.

Asset inventory - what are the assets of this enterprise? Which are the most important assets? What is the level of confidentiality, integrity and availability required for each asset?

User groups and access control - Describe user groups. What data has limited access and which groups have access to it?

Risk analysis - Postulate threat agents who wish to harm the assets of the enterprise. Postulate actions they could take. Estimate likelihood.

Security control selection - For the risks laid out in the risk analysis section, describe security controls to mitigate those risks. Use CIS Top 20 controls as guidance, or another framework if you prefer.

Criteria	Description	Points
Asset Identification	Data assets of the enterprise described. Confidentiality, integrity and availability needs described.	20
Risk Analysis	Threat agents for all assets. Possible actions and likelihood for all threat agent/asset pairs. Well thought out and complete listing of threat/action/likelihood/consequence.	20
User Groups and Access Control	Types of users described, e.g. who are trusted users, what data can they access.	10
Controls	Identify controls for each risk. A framework for the suite of controls, e.g. CIS Top 20, is identified.	20
Writing and Quality	Produce a quality product with correct grammar, free of typos, and	20

	formatted. Put effort and creativity into the product.	
Enterprise	Introduce the enterprise. What is their product or industry. What most important to this enterprise?	5
References	Include references, e.g where you got information on what the threat actors and actions are.	5

Grading Policy

Percent	Grade	Grade Points
93.4 - 100	A	4.00
90.0 - 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00
70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Students Requiring Accommodations
Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation
Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy
UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of

behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment
The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:
• Your academic advisor or Graduate Program Coordinator
• Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
• Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
• Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use
All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy
There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

<u>Health and Wellness</u>

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical support, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall, 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*: https://care.dso.ufl.edu.

On-Line Students Complaints*: http://www.distance.ufl.edu/student-complaint-process.