



DAIENCE UNIVERSITY

Academic Catalog

Volume 1

January 1, 2020 – December 31, 2020

749 Baronne Street, Unit 100-A
New Orleans, LA 70113
(504) 356-0089

www.daience.university

Table of Content

WELCOME MESSAGE	5
OUR VISION	5
OUR MISSION	5
GOALS AND OBJECTIVES	6
ABOUT US	6
RECOGNITION	7
LEGAL CONTROL	7
ADVISORY BOARD	7
ADMINISTRATORS	8
FACULTY	8
HOURS OF OPERATION	11
ACADEMIC CALENDAR	12
MASTER OF SCIENCE IN DATA SCIENCE AND CYBER SECURITY	12
CERTIFICATE COURSES & SEMINARS	12
UNIVERSITY POLICIES	13
ADMISSION REQUIREMENTS	13
ADMISSIONS PROCEDURE	13
ACCEPTANCE TO THE UNIVERSITY	14
NON-DISCRIMINATION POLICY	14
TRANSFER OF CREDIT	15
<i>Transfer into Daience University</i>	15
<i>Transfer out of Daience University</i>	16
<i>Credit for Life Experience</i>	16
STUDENT PRIVACY POLICY	16
STUDENT RECORDS MAINTENANCE	17
IDENTITY VERIFICATION	17
ACADEMIC INTEGRITY	18
CODE OF CONDUCT	19
<i>Prohibitions</i>	19
<i>Sexual and Other Harassment</i>	20
<i>Probation, Suspensions, and Dismissal</i>	21
APPEALS & RE-ADMITTANCE	22

<i>Appeals</i>	22
<i>Re-admittance</i>	22
NON-RETALIATION POLICY	22
COMPLAINT & GRIEVANCE PROCEDURE	23
STUDENT SERVICES	24
<i>Change of Contact Information</i>	24
<i>New Student Orientation</i>	24
<i>Dean's List</i>	24
ACADEMIC POLICIES	26
TECHNOLOGY REQUIREMENTS	26
PROCTORING	27
ATTENDANCE POLICY	27
MAKEUP WORK	27
GRADING	27
<i>Grade Reporting</i>	28
<i>Grade Appeals</i>	28
SATISFACTORY ACADEMIC PROGRESS	29
<i>Academic Warning & Continued Warning</i>	29
<i>Warning</i>	29
<i>Continued Warning</i>	29
<i>Termination</i>	30
<i>Appeals</i>	30
<i>Probation</i>	30
<i>Re-admittance</i>	30
GRADUATION REQUIREMENTS	31
EVALUATION	31
CURRICULUM OFFERINGS	32
MASTER OF SCIENCE IN DATA SCIENCE AND CYBER SECURITY	32
CERTIFICATE COURSES & SEMINARS	40
FINANCIAL INFORMATION	41
TUITION AND FEES	41
CANCELLATION AND REFUND POLICY	41
APPENDIX A	43
CERTIFICATE COURSE SCHEDULE OF OFFERING	43
CERTIFICATE COURSE DESCRIPTIONS	44
APPENDIX B	51

SEMINAR SCHEDULE OF OFFERING	51
SEMINAR DESCRIPTIONS	52

Welcome Message

Welcome to Daience University. Whether you are a current student or considering enrolling in our instruction, we are pleased to have the opportunity to share our institution with you.

The founders created Daience University after discovering a need for qualified IT workers for projects on which they were working. Hiring was—and still is—a challenge, especially in areas like the Middle East, Far East, and Africa. And while there are universities in these areas that teach IT, the infrastructures of these institutions do not always allow for flexibility or innovation.

Thus, the idea for Daience University was born.

Daience University thrives on providing accessible, quality IT education via distance learning, with innovative support services that encourage collaboration and minimize the digital divide. Our university serves students globally, creating an environment for students that will closely mimic the work environment of diverse, multinational teams that they will encounter in the industry.

We hope you are as excited about Daience University, as we are to have you here.

On behalf of the faculty, staff, and myself, welcome and best wishes for you success—both here and beyond.

Mohammad Alkhudari
CEO, Daience University

Our Vision

In the ever-changing IT field, Daience University seeks to be recognized as a quality partner to industry and a quality education provider to students, using technology along with an innovative approach that integrates data science into curriculum with various industry focuses, that will provide students with in-demand skills aligned to both meet current and future industry needs. This unique approach will allow our graduates to get into the growing field of data science with knowledge built around Data Science applications for specific Industries

Our Mission

The mission of Daience University is to provide industry relevant training with a focus on data science techniques combined with a practical application that enables students to increase their skills and expand their knowledge. Daience University seeks to fulfill its mission by offering affordable, quality distance education programs, providing access and opportunity globally and creating a diverse learning community.

Goals and Objectives

Daience University measures the achievement of its missions by the following goals and objectives:

- G1 Provide affordable, accessible education to students around the world
 - O1 Maintain low student cost while remaining financially stable
 - O2 Incorporate distance learning technologies in all program offerings
- G2 Offer quality education offerings that reflect current industry needs
 - O1 Maintain and utilize a program relevant advisory board
- G3 Deliver training to students on a secure platform that facilitates student learning and engagement
 - O1 Maintain a safe and secure online environment that facilitates learning
 - O2 Promote online interaction through course activities
- G4 Create a global community
 - O1 Recruit and enroll qualified students worldwide
 - O2 Promote sharing with respect within diverse student population
- G5 Commit to ethics in all aspects of the education experience
 - O1 Demonstrate transparency and ethical standards in all information shared with prospective students, students, and graduates in all marketing and communications
 - O2 Maintain compliance with all regulatory requirements
- G6 Provide qualified support to students in all aspects of the educational experience
 - O1 Hire qualified faculty to support students in achieving their educational goals
 - O2 Provide student support personnel and activities that align with the size of the institution
- G7 Commit to ongoing evaluation and improvement to support long-term institutional sustainability
 - O1 Collect and use feedback from student, graduates, and stakeholders to make improvements

About Us

Daience University is a 100% online university, headquartered in New Orleans, Louisiana.

Daience University
749 Baronne Street, Unit 100-A
New Orleans, LA 70113

Phone: (504) 356-0089
Email: info@daience.university
URL: www.daience.university

Recognition

Daience University is currently licensed by the Board of Regents of the State of Louisiana. Licenses are renewed by the State Board of Regents every two years. Licensed institutions have met minimum operational standards set forth by the state, but licensure does not constitute accreditation, guarantee the transferability of credit, nor signify that programs are certifiable by any professional agency or organization.

Legal Control

Daience University is 100% owned by Sabaa for Data Science, Inc., an S-Corp incorporated in the State of Delaware.

Advisory Board

Dr. Samer Samarah is a full professor in the Computer Information Systems Department at Yarmouk University, Jordan. He obtained his PhD in Computer Science from the University of Ottawa, Canada in 2008. Dr. Samarah has many published journals and conferences in the area of data science, data mining and IoT. His research focuses on discovering behavioral patterns from data collected by Wireless Sensor Networks and Vehicular ad-hoc Networks. Dr. Samarah is a referee for many international journals and conferences and served as an external examiner for many of these.

Dr. Ali Shatnawi is a full professor in the Department of Computer Engineering at the Jordan University of Science and Technology, where he has been a faculty member since 1996. He had completed his Ph.D. at Concordia University Montreal - Canada, his master and bachelor degrees at Jordan University of Science and Technology - Jordan. His research interests include Data Flow Graphs, High-Level Synthesis, Computer Architecture, Deep Learning and Task Scheduling.

Administrators

Name	Title	Contact
Mohammad Alkhudari	Chief Executive Officer (CEO)	mohammad.alkhudari@daience.university
Dr. Gregory Brown	President	gregory.brown@daience.university
Dr. Ammar Yousef	Chief Financial Officer (CFO)	ammar.yousef@daience.university
Anne Ingleson	Admissions & Student Support Coordinator	anne.ingleson@daience.university
Zaid Bata	Marketing Officer	zaid.bata@daience.university
Esraa Ibrahim	Coordinator	esraa.ibrahim@daience.university
Renad Abdullah	Operation Officer	renad.abdullah@daience.university
Laith Dodin	Operation Administrator	laith.dodin@daience.university
Tala Zaiter	Academic Affairs Coordinator	tala.zaiter@daience.university

Faculty

Name	Title	Qualifications	Contact
Dr. Ali Shatnawi	Chief Academic Officer (CAO), Dean of Data Science and Cyber Security Program	PhD, Electrical and Computer Engineering, Concordia University – Montreal MSc, Electrical Engineering, Jordan University of Science and Technology BSc, Electrical Engineering, Jordan	ali.shatnawi@daience.university

		University of Science and Technology	
Dr. Ahmad Al-Omari	Faculty, Data Science and Cyber Security Program	<p>PhD, Computer Information Systems, Arab Academy for Business and Financial Services</p> <p>MS, Computer Science, University of Jordan</p> <p>BS, Computer Science, Yarmouk University</p>	ahmad.al-omari@daience.university
Dr. Mohammed N. AL-Refai	Faculty, Data Science and Cyber Security Program	<p>PhD, Computer Science, Amman Arab University for Graduate Studies</p> <p>MSc, Computer Science, Al-albayt University</p> <p>BSc, Computer Science, Mu'ta University</p>	mohammed.al-refai@daience.university
Dr. Ziad A. Al-Sharif	Faculty, Data Science and Cyber Security Program	<p>PhD, Computer Science, University of Idaho</p> <p>MS, Computer Science, New Mexico State University</p> <p>BSc, Computer Science, AL al-Bayt University</p>	ziad.al-sharif@daience.university

<p>Dr. Raed Bani-Hani</p>	<p>Faculty, Data Science and Cyber Security Program</p>	<p>PhD, Electrical and Computer Engineering, University of Missouri</p> <p>MS, Computer Engineering and Computer Science, University of Missouri</p> <p>BSc, Electrical Engineering, Jordan University of Science & Technology</p>	<p>raed.bani-hani@daience.university</p>
<p>Dr. Samer Samarah</p>	<p>Faculty, Data Science and Cyber Security Program</p>	<p>PhD, Computer Science, University of Ottawa</p> <p>MSc, Computer Science, Yarmouk University</p> <p>BSc, Computer Science, Yarmouk University</p>	<p>samer.samarah@daience.university</p>
<p>Dr. Mohammad Satti</p>	<p>Faculty, Data Science and Cyber Security Program</p>	<p>PhD, Computer Engineering (ICT Security), Deakin University Geelong</p> <p>BEng, Electrical Engineering, University of New South Wales</p> <p>CEng, Electrical, IT, and Telecom, Institute of Engineers</p>	<p>mohammad.satti@daience.university</p>

Dr. Mohammed GH. I. AL Zamil	Faculty, Data Science and Cyber Security Program	PhD, Information Systems/Data Science, Middle East Technical University MSc, Computer and Information Sciences, Yarmouk University BSc, Computer Science, Yarmouk University	mohammed.al-zamil @daience.university
---------------------------------	---	---	--

Office hours are scheduled based on availability. Students may request a meeting by contacting their instructor.

Hours of Operation

The administrative offices of Daience University are open Monday – Friday between the hours of 9 am and 5 pm US Central Time.

The University observes the following holidays:

- New Year's Day
- Martin Luther King Day
- President's Day
- Good Friday
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving
- Christmas Eve
- Christmas Day
- New Year's Eve

Though the administrative office is closed, students can still access their online courses on these days.

Academic Calendar

Master of Science in Data Science and Cyber Security

The M.S. in Data Science and Cyber Security is normally completed in four (4) terms. During each term, students take three (3) three semester credit hour courses, for a total of nine (9) semester credit hours per term.

Terms begin annually in the Winter, Spring, and Fall. Students may begin the program in any term. The application and enrollment deadlines, along with the term start and end dates, are as follows:

Fall Term 2020

Application Deadline: July 20th

Enrollment Deadline: August 17th

Term Start Date: August 31st

Term End Date: December 18th

Please see the program curriculum for the schedule of courses offered in the 2020 Academic year.

Certificate Courses & Seminars

Please see Appendix A for the Certificate Course schedule of offerings and/or Appendix B for the Seminar schedule of offerings.

University Policies

Admission Requirements

Daience University strives to enroll all qualified applicants who have the desire to learn about data science and cyber security, to begin or enhance their career potential, and the commitment to engage in 100% online studies.

Master of Science in Data Science and Cyber Security

Applicants for admission must have a bachelor's degree or equivalent four-year degree. Additionally, international students may be required to provide TOEFL, IELTS, or PTE exam scores to demonstrate English language proficiency.

Certificate Courses

Applicants for admission must have a high school diploma or the equivalent. Additionally, international students may be required to provide TOEFL, IELTS, or PTE exam scores to demonstrate English language proficiency.

Seminars

There are no admissions requirements for seminars.

Admissions Procedure

Daience University accepts applications on an ongoing basis. Complete applications received before the deadline are evaluated for the next term start date. Incomplete applications cannot be evaluated for admission. Applicants are advised to ensure that all required elements are included with their applications in order to avoid a delay in the admissions process.

Applicants must submit:

1. A completed Application Form
2. Official transcripts verifying completion of:
 - a. a Bachelor's degree or equivalent 4-year degree (Master program only)
 - b. High School or the equivalent (Certificate programs only)
3. A close-up copy of an official government ID or passport; and
4. A photo of the applicant holding the official government ID
5. Application fee

Additional requirements for international students:

1. Transcripts: If the transcript is in a language other than English, an official translation must be included. All international transcripts must be submitted with all components listed in the [World Education Service](#) (WES) Required Documents standards. Applicants are NOT required to submit any documents to WES for translation, but rather, use their standards as a guideline to assure all required transcript components are uploaded and submitted with the application.
2. Proof of English Language Proficiency: Passing an English language proficiency exam is required of applicants whose native language is not English. The only exception is for applicants who have earned a degree at an institution where the language of instruction is English.

For admission, non-native English speaking applicants must score at or above the following levels in one of the following English language proficiency tests:

- Test of English as a Foreign Language (TOEFL PBT), paper-based test: 530
- Test of English as a Foreign Language (TOEFL iBT), internet-based test: 71
- International English Language Test (IELTS): 6.5
- PTE Academic (PTE): 50

Applicants who have already taken the TOEFL, IELTS, or PTE exam can upload a copy of their exam results within the application.

Applicants who have not taken either the TOEFL, IELTS, or PTE exam will need to take it prior to submitting an application to Daience University. Applications cannot be reviewed without qualifying exam results.

Acceptance to the University

Applications are reviewed first by admissions staff and second by the Chief Academic Officer. If it is determined that the application meets all minimum requirements, the applicant will be accepted into Daience University and can start classes in the next term (see Academic Calendar).

Successful applicants will be notified via email. Accepted students sign an enrollment agreement and submit a copy of a government issued photo ID.

Students access the enrollment agreement using the account created to complete the application process. The enrollment agreement is submitted to Daience University electronically by the student. Daience University accepts the enrollment agreement, verified by the signature of the President. The fully executed enrollment agreement is made available to the student as a PDF.

Non-discrimination Policy

Daience University does not discriminate against any person on the basis of age, ancestry, color, ethnic group identification, national origin, religion, race, gender or sex, sexual orientation, physical or mental disability, veteran status, or on the basis of these perceived characteristics, or based on association with a person or group with one or more of these actual or perceived characteristics.

Daience University is committed to compliance with the Americans with Disabilities Act (ADA) of 1990, as amended, and Section 504 of the Rehabilitation Act of 1973, as amended.

Students requiring learning accommodations resulting from disability or injury should contact Support. Daience University provides accommodations based on medical or professional documentation submitted by the student. It is the student's responsibility to self-identify to the institution prior to the start of class.

Transfer of Credit

Transfer into Daience University

The acceptance of transfer credits between institutions lies within the discretion of the receiving institution. Credits earned at other institutions may or may not be accepted by Daience University. Likewise, credits earned at Daience University may or may not be accepted by another institution depending upon its programs, policies, and regulations.

Transfer credits will be evaluated using the following guidelines:

- Only credits earned at an institution that is accredited by an agency recognized by the United States Secretary of Education and/or the Council for Higher Education Accreditation (CHEA), or an accepted foreign equivalent that is listed in the International Handbook of Universities will be considered. Any credits earned at a foreign institution must have a credential evaluation completed indicating equivalency with Daience University courses.
- An official transcript of the student's coursework must be furnished directly by the institution where the coursework was completed before any application for transfer credits can be evaluated.
- A copy of the catalog or course syllabi from the institution at which the coursework was completed, at the time that the coursework was completed, must be furnished before any application for transfer credits can be evaluated.
- A minimum grade of "B" or "3.0" must have been awarded for each course completed to be eligible for transfer. Only courses in which grades were assigned will be considered. Credits earned as a result of a "pass/fail" option are not eligible for transfer.
- Coursework completed more than three years ago is not eligible for transfer of credit.
- Transfer of credit must be completed prior to enrollment. Submitting an official transcript in a timely manner is the sole responsibility of the student.
- The Chief Academic Officer shall make a final determination on the acceptability of transfer credits. The above guidelines shall be used in evaluating all applications for transfer of credit; however, the institution reserves the right to accept or reject any or all transfer credits at its discretion.

Up to 50% of the program can be completed via transfer of credit. Therefore, the maximum number of credits that can be transferred into the Master of Science in Data Science and Cyber Security is eighteen (18) credits or the equivalent of six (6) three-semester credit hour courses.

Students wishing to receive credit for courses taken at other institutions will need to provide all required documents as part of the application process.

Transfer out of Daience University

Transferability of credits earned at Daience University is always up to the discretion of the receiving institution. Daience University does not in any way imply or guarantee the transferability of credit into any other college or university.

Credit for Life Experience

Daience University does not offer credit for life experience.

Student Privacy Policy

Daience University's student privacy and confidentiality policy follows the [Family Educational Rights and Privacy Act \(FERPA\)](#) guidelines.

FERPA was designed to protect the privacy of educational records, to establish the rights of students to inspect and review their educational records, and to provide guidelines for the correction of inaccurate or misleading information through informal and formal hearings.

Daience University will not disclose students' education records without obtaining prior written consent, except in certain instances where a student's educational records may be disclosed to school administrators with a legitimate interest. These individuals may include persons whom Daience University has employed or contracted with, whose responsibility justifies access to all or part of an educational record for legal, educational, or administrative functions.

Students may inspect and review their own records pertaining to academic standing and other information at any time. Students may also seek amendment of inaccurate or misleading information in their education records.

Daience University depends on the accuracy of the records submitted by its students. False information on an application as well as any act to intentionally mislead or misinform instructional personnel or administrators is grounds for disciplinary action, including dismissal from the University. Students seeking access or amendment to their educational records should contact Support.

Student Records Maintenance

Daience University maintains comprehensive records on all students who enroll in its program. The records are maintained in the Student Information System (SIS), which is hosted on the Amazon Web Services infrastructure and served exclusively over SSL. Records are backed up nightly.

Student records include:

- Personal Information (address, email, etc.)
- Enrollment Agreement

- Student initiated petitions/forms
- Course Enrollment and Completion
- Grades Received
- Disciplinary Actions (Warning(s), Probation(s), conduct violations, etc.)
- Progress Evaluations
- Degree Conferred/Diploma
- Transcript

Student records are maintained actively during the enrollment period. Records are archived once a student graduates, is terminated, or otherwise exits Daience University.

Archived records are maintained for 20 years.

Identity Verification

Daience University's Student Identity Verification process begins with the submission of documents during the application process and continues through to a student's graduation, transfer, or withdrawal from the institution.

All students at Daience University must verify that the student registering for a course is the same student who participates in the program and receives credit. In verifying the identity of students who participate in coursework, Daience University may make use of a variety of methods including but not limited to:

1. Receipt of official transcript and government issued photo id;
2. A secure login and authentication process;
3. Proctored examinations; and
4. Other technologies and practices that are effective in verifying student identification.

To ensure appropriate and secure access to the online learning environment, students are responsible for providing complete information about themselves in any identity verification process, in accordance with the Code of Conduct. All methods of verifying student identity protect the privacy of student information in accordance with the Family Education Rights and Privacy Act (FERPA) and any other applicable laws or regulations regarding the confidentiality of personally identifiable information.

All users of Daience University's online learning environment are responsible for maintaining the security of usernames, passwords and any other access credentials assigned, and are responsible for changing passwords periodically to maintain security.

Personally identifiable information may be used, at the discretion of Daience University, as the basis for verifying a student's identity. Students who request that

their passwords be reset may be asked to provide two or more pieces of information for comparison with data on file with Daience University including, such as a social security or government ID number, date of birth, address, and/or email address on file.

Academic Integrity

Commitment to the principles of academic honesty and integrity is essential to the mission of Daience University. In order to maintain an academic climate that is conducive to each student's success, Daience University has established a set of policies and standards.

All work submitted in a course must be the student's own work. The knowing submission of another's work represented as that of the student without properly citing the source of the work will be considered plagiarism. Consequences for plagiarism include: receiving a failing grade on the assignment and being placed on academic probation, receiving a failing grade in the course and being placed on academic probation, or being dismissed from Daience University. The consequences will be determined by and at the discretion of the Chief Academic Officer in consultation with the President and/or faculty members.

In making this determination, Daience University may conduct an investigation to review past homework assignments submitted by the student and reserves the right to change past grades if plagiarism is subsequently found in previous assignments. The submission of the same work to multiple courses violates academic integrity unless substantially changed or cited as previous work. The submission of work completed by others violates academic integrity.

Students who are accused of academic dishonesty can appeal the determination to the Chief Academic Officer. Appeals must be made in writing and include supporting documentation. The Chief Academic Officer will review the appeal and documentation in consultation with the President and/or faculty members, as needed, and make a final decision on the academic dishonesty determination within five (5) days. Students will be notified of the decision on appeals in writing and all documentation will be added to the student's record.

Code of Conduct

The Student Code of Conduct sets forth the standards of conduct expected of students at Daience University. This code is not exhaustive, and students may be subject to disciplinary actions for other behavior and/or activities deemed unacceptable or disruptive to the goals and mission of Daience University.

Students who violate these standards will be subject to disciplinary actions including, but not limited to, issuance of a warning, probation, termination, or

permanent expulsion. Any and all disciplinary action will be recorded in the student's academic record.

Prohibitions

- All forms of academic dishonesty including, but not limited to, cheating, fabrication, facilitating academic dishonesty, and plagiarism.
- Use of any religious, inflammatory or flagrant language in the online learning environment, including discussion boards.
- Use of any religious, inflammatory, or flagrant language related to Daience University on social media or on Daience University social media accounts.
- Misrepresenting oneself as an official Daience University spokesperson online or on social media.
- Engaging in a consensual romantic or sexual relationship with a Daience University faculty or staff member while enrolled at Daience University.
- Endangering, threatening, or causing harm to any member of the Daience University community, causing reasonable apprehension of such harm or engaging in conduct or communications that a reasonable person would interpret as a serious expression of intent to harm.
- Impersonation of another, using another person's identity, or furnishing materially false information, including manufacturing or possession of false identification.
- Forgery, fabrication, falsification, unauthorized alteration, or misuse of university documents, records, or identification.
- Unauthorized use of university property and/or resources.
- Unauthorized access to, disclosure of, or use of any university document, record, or identification including, but not limited to, electronic software, data, and records.
- Interfering with or disrupting university or university-sponsored activities.
- Misuse, theft, misappropriation, destruction, damage, or unauthorized use, access, or reproduction of property, data, records, equipment or services belonging to the university or belonging to another person or entity.
- Engaging in retaliation, harassment or repeated contact that a reasonable person would understand to be unwanted, including, but not

limited to, stalking and/or sexual harassment.

- Engaging in any discriminatory activities as prohibited by applicable law or university policy.
- Interfering with any university disciplinary process.
- Engaging in any illegal sexual offense, including, but not limited to, sexual assault, public sexual indecency, or indecent exposure.
- Violation of any other university policy.
- Conduct that is illegal under state or local law.

Sexual and Other Harassment

Daience University is committed to providing an educational environment free of sexual harassment. Daience University policy prohibits sexual harassment and harassment based on pregnancy, childbirth or related medical conditions, race, religious creed, color, gender, national origin or ancestry, physical or mental disability, medical condition, marital status, registered domestic partner status, age, sexual orientation or any other basis protected by federal, state or local law or ordinance or regulation.

Daience University's anti-harassment policy applies to all students, as well as to all faculty, staff, and administrators involved in the operation of Daience University. It also prohibits harassment based on the perception that anyone has any of the above described characteristics or is associated with a person who has or is perceived as having any of those characteristics.

Prohibited harassment includes, but is not limited to, the following behavior:

- Verbal or written conduct such as epithets, derogatory jokes or comments, slurs or unwanted sexual advances, invitations or comments;
- Visual displays such as derogatory and/or sexually oriented posters, photography, cartoons, drawings, or gestures;
- Physical conduct including assault, unwanted touching, intentionally blocking normal movement or interfering with work because of sex, race or any other protected basis;
- Retaliation for reporting or threatening to report harassment.

Probation, Suspensions, and Dismissal

Students who violate any part of Daience University's Code of Conduct are subject to disciplinary action, including probation, suspension, and dismissal.

Students who have been found to be in violation of the code will be notified via email. The notice will include details regarding the violation and the associated consequence.

During a probation, students are allowed to continue in the program. While under probation, students will be watched closely for additional violations of the Code of Conduct, as outlined in the notification letter. Students who do not violate the code of conduct during the probation period will be placed back into good standing. Students who make further violations will be suspended or dismissed from Daience University.

During a suspension, students are prohibited from continuing their program for one (1) to two (2) sessions, as indicated in the notification letter. Once the suspension has ended, students will rejoin the program on probation, and be watched closely for further violations of the Code of Conduct. Students who do not violate the code of conduct during the probation period will be placed back into good standing. Students who make further violations will be dismissed from Daience University.

Depending on their severity, some violations will lead to immediate dismissal. Though this list is not exhaustive, students found cheating, harassing other students, or participating in illegal activities may be terminated from Daience University immediately. Students expelled for these reasons will not be readmitted.

All disciplinary actions are subject to an appeal. Please see the appeals section for policy details.

Appeals & Re-admittance

Appeals

Within ten (10) days of receiving notification of probation, suspension, or dismissal (academic or non-academic) from Daience University, the student may file a written appeal to the Chief Academic Officer. The Chief Academic Officer will make a decision on the appeal and notify the student of the decision within ten (10) days.

If the appeal is denied, or if the Chief Academic Officer does not respond within ten (10) days after receiving the appeal, the student may appeal directly to the

President. The President shall render a final decision within ten (10) days of the receipt of the appeal.

Re-admittance

A student who has withdrawn from Daience University or who has been dismissed must reapply to Daience University with a new application and go through the admissions evaluation process to enroll. The requirements for the program in effect at the time of the new enrollment will apply.

Daience University will consider past academic records, remedial work done subsequently, and other extenuating circumstances when evaluating re-admission. Any applicant who was previously academically dismissed may, at the discretion of the Chief Academic Officer, be readmitted on probation status. The probation status will extend through one evaluation period (one course). If there are no academic or non-academic violations during the probation period, the student will be returned to good standing. If there is a subsequent violation during the probation period, the student will be terminated and barred from future enrollment at Daience University for a period of not less than three (3) years.

Non-retaliation Policy

Daience University is committed to operating with integrity and maintaining learning and working environments that are free from discrimination and harassment. Retaliation is any action, statement or behavior that is designed to punish an individual for filing a complaint of discrimination or harassment, participating in an investigation, appeal or grievance, or reporting a case where members of the Daience University community are not complying with our policies. Retaliation is an infraction and strictly prohibited.

Students who are aware of or have been subjected to retaliation should promptly report the matter immediately to the Chief Academic Officer who will work with the student to file a complaint. Violators of this policy shall be subject to appropriate disciplinary proceedings as set forth in the Code of Conduct, and may be subjected to sanctions including, but not limited to, probation, suspension, and or termination.

Students who knowingly file a false report will be subject to disciplinary action which may include, but not limited to, probation, suspension, and or termination.

Complaint & Grievance Procedure

A grievance is a serious complaint that demonstrates that the student has been or is being adversely affected by 1) inappropriate interpretation of Daience University policies or 2) inappropriate response, lack of response, or decision by any person with administrative control and responsibility. A grievance is directed

toward Daince University, not a specific person, and should be in writing per the grievance procedure below.

In the event that a student has a complaint, grievance or dispute with Daince University regarding procedures, decisions, or judgments, that cannot be resolved through informal channels, the student has a right to seek a satisfactory resolution through the formal avenues of appeal and redress as follows:

- Step 1 - Notification: The student must notify the relevant faculty member, staff, or administrator in writing, by certified or registered mail postmarked no later than fifteen (15) days after the occurrence, stating the basis for the grievance, the details of the matter, and the remedy requested. The individual so notified shall respond with a decision in writing within fifteen (15) days of receipt of the grievance.
- Step 2 - Appeal: If the remedy requested is denied, or if the notified Daince University faculty member, staff member, or administrator does not respond within fifteen (15) days after the notification of Step 1 has been mailed, the student may appeal in writing, sent by certified or registered mail, directly to the Chief Academic Officer within an additional fifteen (15) day period. The recipient of the appeal will review the grievance and render a decision within fifteen (15) days of receipt of the student's appeal. However, failure to initiate a Step 2 appeal within the fifteen (15) day time frame indicates that the student accepts the Step 1 decision as final and that the matter is closed.
- Step 3: Final Decision. If the remedy requested is denied or the University does not respond within fifteen (15) days after the Step 2 notice has been mailed, the student may appeal in writing, sent by certified or registered mail, directly to the President within an additional fifteen (15) day period. The President will meet with the individuals involved to investigate the matter and will render a decision within fifteen (15) days of receipt of the student's appeal.

The President's decision shall be final. However, failure to initiate a Step 3 appeal within the 15-day period indicates that the student accepts the Step 2 decision as final and that the matter is closed.

If a student has exhausted the complaint and grievance procedure at Daince University and still feels that the issue has not been satisfactorily remedied, the student may file a complaint about this institution with the Louisiana Board of Regents.

Student Services

Change of Contact Information

It is the responsibility of the student to ensure that their contact information is both current and accurate. If, during their enrollment at Daience University, a student's address, phone number, and/or email address changes, the student should update his/her contact information immediately, in the student learning portal.

If a student's name changes (ex: marriage, etc.), the student must contact Daience University to make an update to the student's account. Proof of the name change must be provided by the student.

New Student Orientation

To build a foundation for student success, each student is expected to work through a non-credit orientation prior to beginning the first course. Daience University views the information provided in the orientation to be critical to the student, and therefore, completion of the orientation is required.

The orientation provides the student with details on how to navigate the site, introduces available tools and resources, covers important student policies, reviews writing guidelines, and identifies where students should go for assistance during their studies. If, during a course, a student is not showing familiarity with the information provided in the orientation, he or she may be asked to repeat the orientation by a faculty or staff member.

The Orientation can be found in the student learning portal.

Dean's List

To promote academic excellence, Daience University recognizes degree program students who earn a GPA of at least a 3.8 at the end of each term. These students are recognized on the Dean's List, which is published on the Daience University website.

Career Services Portal

Daience University does not offer formal job placement services. However, the university recognizes that many students are seeking education to enhance their current job skills or to earn skills to start a career or even to change job fields. To facilitate this desire, Daience University connects its graduates with employers who are seeking new talent through the Career Services Portal.

Daience University seeks to build relationships with industry employers all over the globe. Employers are provided access to the Career Services Portal, where they

can post open positions. Graduates can view jobs and apply through the portal. Additionally, graduates can post their CVs in the portal, enabling industry employers to view it and contact the graduate directly through the portal.

All information and activity within the portal is private. Further, the use of the Career Services Portal is not required; it is an optional benefit available to graduates.

Daience University does not guarantee job placement.

Academic Policies

Technology Requirements

At Daience University, electronic communication is the preferred medium for students, faculty, and staff. To take advantage of this technology, it is required that students, faculty, and staff acquire and maintain e-mail access with the capability to send and receive attached files.

In order to navigate the Internet, it is recommended that the latest version of one of the following browsers be used:

- Mozilla Firefox
- Google Chrome

Daience University also provides documents that can be accessed using Adobe Acrobat Reader, which is available without cost to students at www.adobe.com.

Daience University strives to prevent the spread of computer viruses by employing the latest virus detection software on all university-owned computer systems; however, Daience University makes no guarantee related to the unintentional propagation of computer viruses that may go undetected by our virus detection software.

Daience University will not be held liable for any direct, indirect, incidental, special, consequential or punitive damages of any kind, including but not limited to: loss of data, file corruption, or hardware failure, resulting from the effect of any malicious code or computer virus unintentionally transmitted by university staff members, faculty, students or affiliates.

Daience University strongly recommends and urges all faculty and students to seek out and install adequate virus detection software and to routinely check for, and install, the most recent updates to their anti-virus software no less frequently than once each month for their computer and operating system.

Technical Specifications and Instructions

In general, students access course materials using a computer or laptop (PC or Mac), a modern web browser, and a high-speed Internet connection.

Daience University does not support the use of tablets, smartphones or other similar devices for taking any of the courses in the program. While some course material might be accessible on those devices, students are likely to encounter technical issues that may prevent them from successfully completing courses.

Specific courses may have additional technology requirements as specified in individual course syllabi.

Proctoring

All students at Daience University must participate in proctored activities prior to graduation. Proctored activities include exams and presentations. Students taking a course that has a proctored exam must complete the proctored exam to pass the course. Information about proctoring will be provided to students in the courses where it is required.

Attendance Policy

In order to achieve academic success, students at Daience University are expected to attend online lectures and participate in class activities.

In the online learning environment, attendance is defined as:

- Attending synchronous class lectures.
- Logging into the online learning environment at least once per week.
- Completing academic engagement activities as defined on the syllabus e.g. quizzes, discussion, etc.
- Checking email regularly for notices.

Specific attendance policies are included on each course syllabus.

Tardies & Absences

As students are able to login to the online learning environment as their schedules permit, Daience University does not track tardies or absences.

Unsatisfactory Attendance

Students who have not logged into the online learning environment submitted an assignment, taken an assessment, or participated in the discussion board for fourteen (14) consecutive calendar days will be withdrawn from the course which has not been attended.

Makeup Work

All assignments are due as noted on the course syllabus. If a student cannot complete an assignment or activity on or before the due date, he or she must submit a make-up plan. If accepted, DU will allow the student to make up the work by the deadline on the approved make-up plan or the last day of the course, whichever occurs first.

Grading

At Daience University, letter grades are awarded in accordance with each student's demonstration of the prescribed learning objectives and outcomes of each course as follows:

<u>Score</u>	<u>Letter Grade</u>	<u>GPA Points</u>
90-100	A	4.0
80-89	B	3.0
70-79	C	2.0
60-69	D	1.0
0-59	F	0.0

Students may also receive the following designations, as appropriate, which do not receive any GPA points:

- **W** (Withdrawal): Students may withdraw from a course before the end of the third (3rd) week by notifying the instructor.
- **TC** (Transfer Credit): Semester credit granted for semester credits accepted in transfer from other institutions.
- **R** (Repeated Course): Students have the option of retaking a course if they want to improve an unsatisfactory grade. Once a letter grade is recorded for the repeated course, the original grade will be replaced by an "R" grade. The grade points earned from the later grade will be used in computing the cumulative grade point average. A maximum of two courses can be repeated for a better grade during the program. The *original* grade will be replaced with an "R" and excluded from GPA calculation, whether it is better or worse than the new grade. There is no guarantee of a better grade when a student repeats a course.

Daience University faculty may choose to use a performance-based grading component within a course. The course syllabi provide more information about this option and all other course specific grading information including a comprehensive list of graded assignments, assessments, and related weighting.

Grade Reporting

Instructors will report final grades within seven (7) business days of the end of a term. Grades will be reported in the online learning environment.

Students can access their grade reports by using their individual login id and password.

Grade Appeals

Students who believe they have been graded unfairly may appeal their final course grades. The burden of proof in appealing a grade rests with the students. For a change in grade to be recommended, students must show that the grade originally given was unjustly or unfairly awarded.

1. To appeal a grade, students must contact Support within five (5) days of final course grades being reported in the Student Management System.

The appeal must explain why the grade received was incorrect and include supporting evidence.

2. Support will review the appeal and discuss the appeal with the course instructor within five (5) days. The instructor will make a recommendation to Support on whether or not the grade should be changed.
3. Support will provide the instructor's recommendation to the Chief Academic Officer for review. The Chief Academic Officer's review will be completed within five (5) days. The Chief Academic Officer may approve the recommendation or provide an alternate recommendation to the Instructor. If the Chief Academic Officer provides an alternate recommendation to the Instructor, they will discuss it and agree to a final recommendation within five (5) days.
4. The final recommendation, approved by the course instructor and the Chief Academic Officer, will be provided to Support. Support will send a notification to the student of the decision.

Support will change the student's grade, as indicated and place a record of the appeal and final recommendation in the student's file.

Satisfactory Academic Progress

Satisfactory Academic Progress (SAP) evaluations will occur throughout the program, at the conclusion of every three (3) regularly scheduled sessions in a student's enrollment period. At each Progress Evaluation point, Daience University will look to see that the student:

- has satisfactorily completed the minimum number of courses as specified in the table below; and
- has a cumulative GPA of at least a 3.0.

If these criteria are met, students are considered to be in Good Standing. If these criteria are not met, Daience University will begin Academic Probation procedures (see below).

Academic Warning & Continued Warning

Students who do not meet either of the above criteria at any evaluation point will be considered to be making unsatisfactory academic progress and will not be in Good Standing.

Warning

Students who are not in Good Standing will be placed on Warning status and will receive a Warning notification via email. The Warning status will persist through the next evaluation period (three sessions) until the following evaluation point.

During this time, students will be provided an academic improvement plan to make progress toward regaining Good Standing.

Students who fail to show that they are making progress toward regaining Good Standing at the next evaluation point following the Warning period will be placed on Continued Warning. A Continued Warning notification will be sent via email.

Continued Warning

Students on Warning status who do not regain Good Standing during the Warning period, but who show progress toward regaining Good Standing, may be granted one additional evaluation period (three sessions) to continue their academic improvement plan and achieve Good Standing. This additional evaluation period is called Continued Warning.

Progress toward regaining good standing is demonstrated through students raising their Cumulative Grade Point Average (CGPA) toward the minimum 3.0 average and/or showing the ability to complete the program within the maximum time frame of 150%.

Students who fail to achieve Good Standing at the next evaluation point following the Continued Warning period will be terminated from the program.

Termination

Students failing to return to Good Standing at the end of the Continued Warning period will be terminated from Daience University. Students will receive notice of Academic Termination via email and will no longer have access to the online learning environment.

Appeals

Students wishing to appeal Academic Termination determination must do so in writing within ten (10) calendar days of receipt of the email notification.

Appeals should be directed to the Chief Academic Officer. All appeals should be made in writing and include appropriate documentation (e.g. a physician's statement, accident report, evidence of grade miscalculation, etc.) showing that the failure to obtain Good Standing was beyond the student's control. The Chief Academic Officer will notify students of the decision within ten (10) days of receiving the appeal. The Chief Academic Officer's decision is final.

Probation

In cases where an appeal is accepted, that student is placed on Probation status for the next evaluation period (three sessions) through the next evaluation point.

During this time, students will be provided an academic improvement plan to regain Good Standing by the end of the Probation period.

Students not achieving Good Standing at the end of the Probation period will be terminated from Daience University. Termination following Probation cannot be appealed.

Re-admittance

Students whose enrollment at Daience University is terminated due to academic reasons will be eligible for re-enrollment after a waiting period of six (6) months. These students may be eligible to receive credit for courses previously completed at Daience University per the transfer of credit policy.

Graduation Requirements

In order to graduate from Daience University and be awarded a Master of Science in Data Science and Cyber Security, students must:

- Successfully complete all required courses;
- Earn a minimum of 18 credit hours in the program at Daience University;
- Be in academic good standing; and
- Have a cumulative GPA of at least 3.0.

Once graduation requirements have been verified, the student will be notified via email and the diploma made available.

Evaluation

At the end of each course, students are encouraged to complete an end-of-course survey. These surveys are anonymous, so students can submit suggestions and feedback freely. Findings from these surveys are used to improve course content, instruction, and the overall student experience at Daience University.

Curriculum Offerings

Master of Science in Data Science and Cyber Security

Number of Courses: 12

Credit Hours: 36 Semester Credit Hours

Delivery Method: Online

Program Description:

Daience University's Master of Data Science and Cyber Security program prepares professionals to assume cyber security and information assurance leadership roles in corporations, agencies, and organizations with a curriculum rich in computer security management, IT security threat assessment, incident response, organizational management, behavior, and leadership. The program is designed to prepare students to become creators of knowledge and inventors of processes.

The master's degree has been divided into a set of core courses that provide the necessary skills in data science, cyber security, organizational behavior, structure, research, and writing. The program offers select specializations that allow students to focus on a field of study that best meets their individual needs and goals. Each specialization aligns with industry skills and knowledge that have been derived from the NICE framework to enhance career applicability.

The primary objective of this program is to prepare students for supervisory positions in careers requiring extensive understanding and interaction with information system security and crimes. The student's desire for this program comes from the strong relation between the two sectors in areas such as; computer security, Information Systems (IS) strategy and policy, cybercrimes and prevention. The program also prepares the students for the dynamic, expanding world of Big Data and Data Science driven analysis and computation. Another major objective of this program is to prepare students for subsequent studies and research.

The Master of Science in Data Science and Cyber Security program is offered 100% online, providing students with the flexibility to attend classes from anywhere. Students are supported by highly qualified faculty, who provide the fundamental theory and skills needed to perform specific tasks and projects. As a result, they will have an opportunity to contextualize their learning and build skills for future careers or degrees.

Program Learning Outcomes (PLOs):

1. Differentiate the nature of risks and pathways of threats to cyber and cyber-physical systems.

2. Outline vulnerabilities to software, networks, and computer systems.
3. Illustrate the ability to recognize, design and implement efficient software solutions to problems.
4. Employ methods and strategies for protecting data on networks, in software, as well as, other cyber and cyber-physical systems.
5. Evidence the ability to communicate effectively and to work as a team.
6. Attain employment and/or to be accepted into a data science and cyber security PhD. Program.
7. Identify the constraints and costs of cybercrime and espionage to privacy, communication, and use of technology.
8. Summarize the role that government, corporate, and coalition policies can have towards slowing and stopping cybercrime and surveillance.

Intended Learning Outcomes (ILOs)

A. Knowledge and Understanding

Students will be able to:

- A1)** Demonstrate knowledge of a range of advanced topics in Data Science and Cyber Security beyond the undergraduate level and at the forefront of research.
- A2)** Use knowledge and understanding of research methodology and practice.
- A3)** Comprehend, apply and develop leading-edge technologies.

B. Intellectual Skills

Students will be able to:

- B1)** Evaluate original ideas in a research context.
- B2)** Demonstrate problem-solving in academic and industrial environments.
- B3)** Create original ideas in a research context (synthesis).

C. Practical Skills

Students will be able to:

- C1)** Develop applications to satisfy given requirements.
- C2)** Systematize and pursue a scientific or industrial research project.
- C3)** Utilize, manipulate and develop large computational systems.
- C4)** Accomplish independent information acquisition and management.

D. Transferable Skills and Personal Qualities

Students will be able to:

- D1)** Perform and communicate effectively as a team member.
- D2)** Prepare and present seminars to a professional standard.
- D3)** Identify ethical issues related to professional activities.
- D4)** Author a thesis and reports to a professional standard.
- D5)** Implement independent and efficient time-management.

Course Descriptions

Course Number: DSCS701

Course Title: Research and Writing for the IT Practitioner

Credit Hours: 3

Type: Required

Description: The Research and Writing for the IT Practitioner course provides 21st Century IT practitioners with the knowledge and skill to read, understand, implement, and conduct research in the workplace. Emphasis will be placed on data driven analysis, understanding credibility of resources, and determining data validity. Students will design and conduct a research project in the course, write an analysis document, and present their project to other students.

Course Number: DSCS703

Course Title: Programming with Python

Credit Hours:3

Type: Required

Description: Students will learn the core concepts of Python, and more advanced Python programming with a focus on enterprise development, students will learn more advanced Python programming with a focus on enterprise development. Students will use Python to interact with databases and GUI's and perform Network Programming. This is a practical, hands-on course, designed to teach students practical programming for the real business application.

Course Number: DSCS704

Course Title: The Hacker Mind (profiling the IT Criminal)

Credit Hours: 3

Type: Required

Description: Cyberspace has increased human communication, connectivity, creativity, capacity, and unfortunately, crime by leaps and bounds in the last decade. For all of the positive opportunities that the internet and global connectivity provide, it offers as many harmful opportunities for those who seek them. These negative aspects can be used by everyone from the high school challenge hacker to the international terrorist. Businesses, governmental agencies, militaries, and organizations of every kind are threatened by the IT criminal. This course will survey the spectrum of psychological attributes which may make up the profile of the IT criminal so that organizations of all types can work to stay ahead of the game and minimize risk

Course Number: DSCS705

Course Title: Operational Security for Critical Infrastructure

Credit Hours: 3

Type: Elective

Description: Critical Infrastructure is that which continuous operation is deemed necessary to ensure the security of a given nation, its economy, and the public's health and/or safety, like (ESADA and SS7). The Operational Security for Critical Infrastructure course is designed to provide students with the knowledge to manage and operate critical infrastructure surrounding the protection of systems, networks, and assets.

Course Number: DSCS707

Course Title: Linux Networking and Security

Credit Hours: 3

Type: Required

Description: This course focuses on configuring a secure Linux network using command line and graphical utilities. Emphasis is placed on file sharing technologies such as the Network File System, NetWare's NCP file sharing, and File Transfer Protocol. Additional topics include making data secure, user security, file security, and network intrusion detection. Students will be required to take on the role of problem solvers and apply the concepts presented to situations that might occur in a work environment

Course Number: DSCS708

Course Title: Advanced Hacking Techniques

Credit Hours: 3

Type: Required

Description: The Advanced Hacking Techniques course focuses on how perimeter defenses work, how intruders escalate privileges, and methods of securing systems. Additional topics include intrusion detection, policy creation, social engineering, DoS attacks, buffer overflows, and virus creation. Through this course Students will be able to apply hacking tools and methods to maintain access to the system during penetration testing.

Course Number: DSCS710

Course Title: Conducting Penetration and Security Tests

Credit Hours: 3

Type: Elective

Description: The Conducting Penetration and Security Test course focuses on mastery of the international standard for penetration testing. Topics include customers and legal agreements, penetration testing planning and scheduling, information gathering, external and internal network penetration testing, router penetration testing, firewalls penetration testing, intrusion detection system penetration testing, wireless networks penetration testing; password cracking penetration testing, social engineering penetration testing, PDA and cell phone penetration testing, and penetration testing report and documentation writing.

Through this course Student analyzes the differences between ethical and unethical penetration testing by applying different tools and methods to conduct penetration tests and exploit systems during penetration testing

Course Number: DSCS712

Course Title: Building Cyber Architecture

Credit Hours: 3

Type: Elective

Description: In the Building Cyber Architecture course, students will learn about enterprise security, enterprise structure, and enterprise security requirements. Topics include Meaning of Architecture Security, Architecture Model, Systems Approach, Contextual and Conceptual Security Architecture, Logical and physical Security Architecture, Operational Risk Management, and Assurance Management. Through this course, students will be able to use models and apply the return on Investment in Security Architecture. Also, students can use techniques such as defense in depth to demonstrate how controls can be selected, deployed, and tested to minimize risk and impact.

Course Number: DSCS713

Course Title: Secure Programming

Credit Hours: 3

Type: Elective

Description: The Secure Programming course provides the essential and fundamental skills for secure programming. The most prevalent reason behind vulnerabilities and buggy code being exploited by hackers and malicious code is the lack of adoption of secure coding practices. This course will expose students to the inherent security drawbacks in various programming languages or architectures. Further, they will learn strategies to exercise secure programming practices to overcome these inherent drawbacks and preempt bugs from the code.

Course Number: DSCS714

Course Title: Investigating Network Intrusions and Computer Forensics

Credit Hours: 3

Type: Elective

Description: The Investigating Network Intrusions and Computer Forensics course focuses on cyber-attack prevention, planning, detection, and incident response with the goal of counteracting cybercrime, cyber terrorism, and cyber predators, and holding perpetrators accountable. Additional topics include fundamentals of computer forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity, computer security policies and guidelines, and case studies. Upon completion of this course, students will be able to use typical forensic investigation tools and Investigate network security events and incidents using a scientific approach

Course Number: DSCS715

Course Title: Advanced Mobile Forensics and Security

Credit Hours: 3

Type: Elective

Description: The Advanced Mobile Forensics and Security course focuses on the intricacies of manual acquisition (physical vs. logical) and advanced analysis using reverse engineering to understand how popular Mobile OSs are hardened to defend against common attacks and exploits. Topics include; mobile forensic challenges and process, mobile hardware design and architectures, OS architecture, boot process, and file systems, threats and security, evidence acquisition and analysis, application reverse engineering, and mobile forensics reporting and expert testimony. Through this course, students will be able to extract information from mobile devices, and validate the results of mobile forensics solutions, Demonstrate various mobile enabling technologies, forensics process, methods, techniques and tools.

Course Number: DSCS716

Course Title: Cyber Law

Credit Hours: 3

Type: Elective

Description: The Cyber Law course focuses on cyber-attack prevention, planning, detection, and incident response with the goal of counteracting cybercrime, cyber terrorism, and cyber predators, and holding perpetrators accountable. Topics include fundamentals of computer forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity, computer security policies and guidelines, and case studies.

Course Number: DSCS717

Course Title: Incident Handling and Response

Credit Hours: 3

Type: Elective

Description: The Incident Handling and Response course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Emphasis is placed on computer forensics and its role in handling and responding to incidents. Through this course students will become proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, insider attack threats, incident response teams, incident management training methods, and incident recovery techniques in detail.

Course Number: DSCS720

Course Title: Artificial Intelligence

Credit Hours: 3

Type: Elective

Description: The Artificial Intelligence course is divided into four parts. The first part covers knowledge representation. The second part introduces heuristic search and constraint satisfaction. The third part is dedicated to advanced topics such as rule-based Expert Systems, case-based reasoning, and model-based reasoning. Finally, the fourth part is dedicated to machine learning techniques and theory. Through this course students will be able to differ between supervised, unsupervised and reinforcement learning, be exposed to use cases, and see how clustering and classification algorithms help identify AI business applications.

Course Number: DSCS719

Course Title: Risk Management

Credit Hours: 3

Type: Elective

Description: In the Risk Management course, students will examine information security as a risk management problem where the organization identifies information security risks, evaluates those risks, and makes risk mitigation and acceptance decisions given its resource constraints. Part one of this class covers foundational concepts in risk management and economic valuation and will be introduced to standard risk management approaches for identifying, analyzing, and responding to risk, as well as the tools and methodologies for metrics to monitor risk management activities. Part two of the course expands coverage to more quantitative approaches to risk analysis, risk valuation, and risk metrics using Factor Analysis of Information Risk (FAIR) and an associated analysis software toolset called Risk Lens.

Course Number: DSCS721

Course Title: Data Mining

Credit Hours: 3

Type: Elective

Description: The Data Mining course provides a practical and technical introduction to knowledge discovery and data mining. The topics that will be covered include problems of data analysis in databases, discovering patterns in the data, and knowledge interpretation, extraction and visualization. Additionally, data mining and machine learning techniques used for descriptive and predictive analysis, such as clustering association rules mining, classification, prediction, will be covered. This course is an absolute necessity for those interested in joining the data science workforce, and for those who need to obtain more experience in data mining.

Course Number: DSCS722

Course Title: Threat Intelligence

Credit Hours: 3

Type: Elective

Description: The Threat Intelligence course will provide students with an in-depth examination of the cyber threat intelligence cycle, the incident response cycle,

and how they combine to form the Intelligence-driven Incident Response (IDIR) process. Students will use interactive exercises to become familiar with and practice the creation and consumption of Cyber Threat Intelligence products.

Course Number: DSCS725

Course Title: Deep Learning

Credit Hours: 3

Type: Required

Description: Deep learning is a branch of machine learning concerned with the development and application of modern neural networks. Deep learning algorithms extract layered high-level representations of data in a way that maximizes performance on a given task. For example, if asked to recognize faces, a deep neural network may learn to represent image pixels first with edges, followed by larger shapes, then parts of the face like eyes and ears, and, finally, individual face identities. Deep learning is behind many recent advances in AI, including Siri's speech recognition, Facebook's tag suggestions and self-driving cars. This course will cover a range of topics from basic neural networks, convolutional and recurrent network structures, deep unsupervised and reinforcement learning, and applications to problem domains like speech recognition and computer vision.

Course Number: DSCS726

Course Title: Advanced Networking and Data Security

Credit Hours: 3

Type: Required

Description: The Advanced Networking and Data Security course explores the basic components and design principles of advanced broadband networks (wireline and wireless) and how they enable essential services such as mobility, secure data storage, processing and transmission. This course will also introduce the student to emerging issues facing organizations considering implementing cloud computing services and mobility to enable worker productivity. Students will be exposed to the basic pillars of network security (IA) and protecting individual privacy.

Course Number: DSCS727

Course Title: Big Data Analysis

Credit Hours: 3

Type: Required

Description: The Big Data Analysis course provides the data science students with an understanding of the Big Data and its role in data analysis. It provides the terminology and core concepts behind big data problems, applications, and systems. It affords introduction to one of the most common frameworks, Hadoop and Spark, that have made big data analysis easier and more accessible. Also, it will provide you with the necessary skill in manipulating big data distributed over a cluster using functional concepts and in-memory distributed collections

framework written in Scala or Spark. We'll cover Spark's programming model in detail, being careful to understand how and when it differs from familiar programming models, like shared-memory parallel collections or sequential collections. Through hands-on examples in Spark and Scala, students learn when important issues related to distribution like latency and network communication should be considered and how they can be addressed effectively for improved performance.

Course Number: DSCS799

Course Title: Capstone Project

Credit Hours: 3

Type: Required

Description: The Capstone Project course will enable students to apply and coordinate their acquired knowledge, then deepen it through a specified theory-based capstone project. The Capstone Project will allow students to showcase their skills and abilities, use scientific methodology, and showcase their academic competence in various ways in preparation to transition from the academic to the industry environment.

Certificate Courses & Seminars

Please see Appendix A for the Certificate Course descriptions and/or Appendix B for the Seminar descriptions.

Financial Information

Tuition and Fees

Master of Science in Data Science and Cyber Security

<i>Application Fee (non-refundable)</i>	\$75
<i>Registration Fee (non-refundable)</i>	\$200
<i>Library Services Fees</i>	\$30/course
<i>Tuition (per 3 credit hour course)</i>	\$750
<i>Books & Materials Fees</i>	Est: \$50 - \$100/course
<i>Total Projected Cost per Term (USD)</i>	\$2640
<i>Total Projected Cost of Program (USD)</i>	\$10,835

All Certificate and Professional Development/Seminar Courses

<i>Registration Fee</i>	\$50
<i>Tuition</i>	\$150
<i>Books & Materials Fee</i>	\$100
<i>Certification Exam</i>	\$200
<i>Total Cost (USD)</i>	\$450

Cancellation and Refund Policy

Students may cancel their enrollment at Daience University at any time. A student's notification of cancellation may be conveyed to the institution in any manner.

A student has five (5) calendar days after signing an enrollment agreement or similar contractual document to cancel enrollment and receive a full refund of all monies paid to the institution.

A student requesting cancellation more than five calendar days after signing an enrollment agreement, but prior to beginning a course or program, is entitled to a refund of all monies paid minus:

- An application fee of \$75 (if applicable)
- The non-refundable registration fee of \$200 or \$50 (as applicable)
- The non-refundable library services fee of \$30 per course (if applicable)

Upon cancellation, a student whose costs for education are paid in full, but not eligible for a refund, is entitled to receive all materials including kits and equipment.

Tuition will be refunded per the table below. Tuition for courses that have not been started will be refunded in full. There is no tuition refund for courses and/or terms that have been completed.

Length of Term	Tuition Refund Amount	
15 Weeks	1 st Week	80%
	2 nd Week	70%
	3 rd Week	60%
	4 th Week	50%
	5 th Week	40%
	6 th Week	30%
	7 th Week	20%
	8 th Week	10%
	9 th Week	0%

Any refund due to a student will be paid in full within 30 days.

Refund Calculation Example

The refund amount for a student who withdraws from the first term of the Master of Science in Data Science and Cyber Security program during the 3rd week of training would be calculated as follows:

DU Retains:

Application Fee:	\$75
Registration Fee:	\$200
Library Services Fee:	\$30/course
Portion of Tuition:	\$900 (40% x \$2250)
Total Retained by DU:	\$1,265

Student Refund Amount:

Portion of Tuition:	\$1350 (60% x \$2250)
Total Refunded to Student:	\$1,350

Refunds on books and materials are subject to the terms of the retailer from which they were purchased (ex: Amazon).

The student refund amount is applied to any balance on the student's account.

Appendix A

Certificate Course Schedule of Offering

Certificate courses are offered on a quarterly basis, four (4) times per year. Each quarter is eight (8) weeks long.

Quarter Schedule 2020

Quarter 1: January 21st - March 13th

Quarter 2: March 16th - May 8th

Quarter 3: August 24th - October 16th

Quarter 4: October 19th - December 11th

The following certificate courses will be offered during the 2020 Academic Year. Please contact Daience University or see the website for the start and end dates of each program and scheduled class times:

Course Number	Course Name
Quarter 1	
CS-15	Cyber Security Administrator Certificate
DS-16	Data Science for Healthcare Professionals Certificate
DS-19	Data Science for Financial Services Certificate
DS-17	Data Science for Oil & Gas Certificate
DS-18	Data Science for Public Sector Certificate
CS-24	Digital Forensics Certificate

LG-26	English Language 01 Certificate
Quarter 2	
CS-06	Cyber Security Specialist Certificate
DS-08	Data Science for Manufacturing Certificate
CS-09	Cyber Awareness Certificate
LG-27	English Language 02 Certificate
BC-12	Leadership & Foster Partnership Certificate
LG-28	Languages 01 Certificate: Arabic, Chinese, and French
LG-29	Languages 02 Certificate: Arabic, Chinese, and French
CS-01	Penetration Tester Certificate
DS-02	Data Science for Education Certificate
CS-03	Chief Information Security Officer Certificate
CS-04	Security Manager Certificate
Quarter 3	
DS-16	Data Science for Healthcare Professionals Certificate
CS-15	Cyber Security Administrator Certificate
DS-17	Data Science for Petroleum Professionals Certificate
DS-18	Data Science for Public Sector Certificate
CS-13	Security Operations Center Analyst Certificate
DS-19	Data Science for Financial Services Certificate
Quarter 4	
CS-03	Chief Information Security Officer Certificate
DS-02	Data Science for Education Certificate
CS-01	Penetration Tester Certificate
CS-04	Security Manager Certificate

CS-24	Digital Forensics Certificate
LG-26	English Language 01 Certificate
LG-27	English Language 02 Certificate
LG-28	Languages 01 Certificate: Arabic, Chinese, and French
LG-29	Languages 02 Certificate: Arabic, Chinese, and French

Certificate Course Descriptions

Course Name: Penetration Tester Certificate

Course Number: CS-01

Clock Hours: 20

Description: The purpose of the Penetration Tester Certificate course is to give students an essential overview of what to look for when beginning penetration testing. Successful graduates of the course will be able to build an internal penetration test kit for performing both client-side and server-side penetration tests on a company network. The course will also alert students to potential challenges with network technology, such as wireless networks, common web apps, and remote access devices, that can circumvent network perimeter security devices such as firewalls and intrusion detection systems. At the conclusion of this course, students will gain experience in both the capabilities and functionality of penetration testing tools.

Course Name: Data Science for Education Certificate

Course Number: DS-02

Clock Hours: 20

Description: The Data Science for Education Certificate course provides students with training on data collection, storage, administration, visualization, and privacy as it relates to the education industry. Students will practice programming, algorithms, and methods for statistical analysis in data mining and machine learning while utilizing software tools and systems for processing educational data. Successful students will be able to implement these methods in an educational setting while understanding ethical, management, policy and legal requirements in the field of data science.

Course Name: Chief Information Security Officer Certificate

Course Number: CS-03

Clock Hours: 20

Description: Chief Information Security Officers (CISO) lead large-scale IT security departments and are responsible for providing leadership to the overall IT security of an organization. The Chief Information Security Officer Certificate course prepares students for the complexities of this role, including how to develop risk management programs, how to properly respond as an organization to IT threats, and best practices when working with law enforcement and government entities on corporate security matters. This course is designed to bridge the knowledge gap for an existing executive manager who is making the transition to a CISO role. Successful graduates of this course will be able to understand and implement large scale IT security protocols in a corporate setting.

Course Name: Security Manager Certificate

Course Number: CS-04

Clock Hours: 20

Description: Students in the Security Manager Certificate course will gain an understanding of security, resilience and fraud functions that are focused on the protection of a business' brand, employees, assets and data. By utilizing multiple layers of interdependent systems, successful students will be able to implement strategies for IT security that increase the confidence of shareholders, customers, and business stakeholders, by preventing losses, disruptions, and damage to the business. Students will learn how to recognize and respond to IT security threats through management, organization, assessment and investigation techniques.

Course Name: Cyber Security Specialist Certificate

Course Number: CS-06

Clock Hours: 20

Description: Cyber Security Specialists protect information from theft, illegal duplication, and unauthorized access. Students in the Cyber Security Specialist Certificate course will learn how to protect information on computer networks, cloud servers, mobile devices, and financial software. Successful graduates will be able to analyze potential risks, develop strategies to prevent data security breaches, and implement security measures to impede the efforts of cybercriminals across multiple platforms.

Course Name: Data Science for Manufacturing Certificate

Course Number: DS-08

Clock Hours: 20

Description: Modern manufacturing techniques incorporate robotization, automation, and broad application of data. The Data Science for Manufacturing Certificate course teaches students how to use computation to work with massive manufacturing data sets to locate specific results, including the use of data structures, algorithms, parallel computing, data simulation, and

analysis. Successful graduates of this course will be able to implement these data science methods within a large manufacturing setting.

Course Name: Cyber Awareness Certificate

Course Number: CS-09

Clock Hours: 20

Description: In the Cyber Awareness Certificate course, students will learn how to assess the security culture of an organization, then create and implement a plan to improve it. Students will master strategies on how to align an IT program with an organization's goals while earning support from the organization's executive administration. Successful graduates will be able to understand how people learn, how to analyze media consumption, and in turn, how to create marketing campaigns that increase the likelihood of behavioral change in an organization.

Course Name: Leadership & Foster Partnership Certificate

Course Number: BC-12

Clock Hours: 20

Description: The Leadership & Foster Partnership Certificate course enables students to learn about leadership theories and models through skill development exercises. This course links leadership with strategic thinking to promote integrative learning, and the capacity to examine and solve problems from multiple perspectives. Topics covered include decision-making techniques, critical thinking, identifying & hiring talent, organizing & fostering teams, emotional intelligence, financial management, and customer trust and credibility. Successful graduates of this course will be able to implement a leadership style and method best suited for their own professional lives, increasing their capacity to be a leader and an organizational asset in the workplace and beyond.

Course Name: Security Operations Center Analyst Certificate

Course Number: CS-13

Clock Hours: 20

Description: The Security Operations Center (SOC) Analyst Certificate course is designed to develop a student's competency in keeping an organization's proprietary and sensitive information secure. Students will be trained on how to work inter-departmentally to identify and correct flaws in a company's security systems, solutions, and programs while recommending specific measures that can improve the company's overall security against cyber-attacks. Students will learn about the functionality of IT security devices, protocol, ports and services, real-world cyber-attacks, and how to investigate a cyber-attack. Graduates of the course will be able to utilize network packets and device logs to perform the day-to-day activities of a SOC Analyst while being able to identify various cyber-attacks and remediation strategies.

Course Name: Cyber Security Administrator Certificate

Course Number: CS-15

Clock Hours: 20

Description: The Cyber Security Administrator Certificate course trains students on how to properly conduct all aspects of a company's information security. Topics within this course include sources of virtual data resources, security methods for desktop, mobile, and networks, how to install, administer and troubleshoot an organization's security solutions, compliance with ethics and security concepts, asset management, change management duties, and physical security operations and security awareness. Successful students will learn how to perform the various roles of Cyber Systems Administrators, including protocol training with staff, monitoring network traffic, performing risk assessment, auditing machines and their software, updating security patches, and ensuring that each network resource has the proper defenses.

Course Name: Data Science for Health Care Professionals Certificate

Course Number: DS-16

Clock Hours: 20

Description: The Data Science for Health Care Professionals Certificate course provides students with a working knowledge of Real-World Data (RWD) and Real-World Evidence (RWE), and how to utilize both within the healthcare industry. Students will learn current trends in RWE and existing methodologies for using it, including considerations of ethics, design-thinking, commercial applications, and the limitations of RWE. Successful students will be able to complete exercises using RWE, applying user-friendly business intelligence tools to analyze RWD in commercial healthcare, life science pharmaceuticals, healthcare regulation, and biotech and medical device industries.

Course Name: Data Science for Petroleum Professionals Certificate

Course Number: DS-17

Clock Hours: 20

Description: The Data Science for Petroleum Professionals Certificate course teaches students how data science is utilized within the petroleum industry. Course topics include the importance of oil & gas data, data-driven and physics-driven processes, predictive analytics, and how data can be used to proactively track operations and equipment performance. Successful students will be able to apply these topics in a number of petroleum applications, including seismic surveys, drilling equipment sensor data, production & drilling assessment, and other petroleum operations that require analysis of large datasets.

Course Name: Data Science for Public Sector Certificate

Course Number: DS-18

Clock Hours: 20

Description: The Data Science for Public Sector Certificate course is designed to teach students working in the public sector how to utilize data science to drive efficiency in public policy. Course topics include data capture methods, company databases, data collection on the internet, data management and

storage, and presentation methods for data analysis, including report writing, producing visualizations, and policy recommendations. Successful graduates of this course will be able to implement these methods in the public sector, including applications that help deliver better public services, improve transparency, reduce costs and enhance customer service.

Course Name: Data Science for Financial Services Certificate

Course Number: DS-19

Clock Hours: 20

Description: The Data Science for Financial Services Certificate course teaches students how to extract valuable insights from financial data utilizing the Python programming language. Course topics include fundamentals of the Python open data science stack, Python applications to finance, how to collect data from different sources, and fundamentals of machine learning. Successful graduates of this course will develop analytical skills and tools to develop financial modeling or algorithmic trading strategy using Machine Learning.

Course Name: Digital Forensics Certificate

Course Number: CS-24

Clock Hours: 20

Description: The Digital Forensics Certificate course provides students with an overview of the many aspects of digital forensics, which includes data analysis, the examination of personal computers, network forensics, investigating network security breaches, hacking attempts, and data theft. These course topics are discussed and applied in several class exercises, and successful graduates of this course will be able to apply forensic best practices to routine administrative procedures and alert verification, and understand how routine actions can negatively affect the forensic value of data. Additionally, this course will prepare administrators to approach both routine and unusual events in a systematic forensic manner.

Course Name: English Language 01 Certificate

Course Number: LG-26

Clock Hours: 20

Description: The English Language 01 Certificate course teaches students the basics of English descriptive grammar, linguistics, and important terminology used to describe elements of sentences, sentence types, subordinate clauses, adverbs, and the different verb tenses. Students will be able to identify the elements of an English sentence, identify sentence types in English, and identify types of subordinate clauses in complex sentences. Successful graduates of this course will improve their basic ability to read, write, and comprehend the English language in both professional and personal environments.

Course Name: English Language 02 Certificate

Course Number: LG-27

Clock Hours: 20

Description: The English Language 02 Certificate course teaches students to understand a wide range of demanding English texts, recognize implicit meanings, and develop the skills to express yourself fluently and spontaneously in English. Students will practice how to use English flexibly and effectively for social, academic and professional purposes, and will learn how to produce detailed texts that utilize sophisticated organizational structures. Successful graduates of this course will increase their ability to read, write, and comprehend advanced English language in a variety of settings.

Course Name: Languages 01 (Arabic, Chinese and French) Certificate

Course Number: LG-28

Clock Hours: 20

Description: The Languages 01 (Arabic, Chinese and French) Certificate course provides students with a basic knowledge of three different types of language: Arabic, Chinese and French. Student assignments include speaking and listening practice through audio/visual media, interactive activities, and paired dialogue exercises. Language skills are developed through graded reading activities, character writing practice, and composing short pieces for developing writing competency. This course equips students with a strong emphasis on grammar to provide the necessary framework to communicate clearly and effectively. Successful students will achieve beginning levels of fluency in communicating, reading and writing in simplified Arabic, Chinese and French characters.

Course Name: Languages 02 (Arabic, Chinese, and French) Certificate

Course Number: LG-29

Clock Hours: 20

Description: The Languages 02 (Arabic, Chinese and French) Certificate course is designed for students who have been previously exposed to these three languages, and already have a basic knowledge of present, past and future verb tenses. Student vocabulary and phonetics will be enhanced through visual and auditory exercises, and dialogue and oral presentations will help in forming and developing these language skills. Successful graduates of this course will develop a strong grammar foundation through various reading, speaking, writing and listening activities.

Appendix B

Seminar Schedule of Offering

Seminars are offered on a quarterly basis, four (4) times per year. Each quarter is eight (8) weeks long.

Quarter Schedule 2020

Quarter 1: January 21st - March 13th

Quarter 2: March 16th - May 8th

Quarter 3: August 24th - October 16th

Quarter 4: October 19th - December 11th

The following seminars will be offered during the 2020 Academic Year. Please contact Daience University or see the website for the start and end dates of each seminar and scheduled class times:

Seminar Number	Seminar Name
Quarter 1	
BC-20	Entrepreneurship and Internship
BC-21	Innovation Management
BC-22	Creative Thinking

BC-23	Digital Marketing
BC-25	Designing Thinking for Innovation
BC-14	Big Deal Closer
Quarter 2	
BC-05	Fundamentals of Business Communication
DS-07	Cyber Security Fundamentals for Executives
Quarter 3	
BC-14	Big Deal Closer Course
BC-20	Entrepreneurship and Internship
BC-10	Computer Skills
BC-21	Innovation Management
BC-11	Finance for Non-Finance Managers
Quarter 4	
BC-05	Fundamentals of Business Communication
BC-23	Digital Marketing
DS-22	Creative Thinking
BC-25	Design Thinking for Innovation

Seminar Descriptions

Course Name: Fundamentals of Business Communication

Course Number: BC-05

Clock Hours: 15

Description: The Fundamentals of Business Communication seminar provides students with information on listening skills, and techniques to know when to speak, and how to speak clearly and concisely. These skills are critical in business communication and will assist students in becoming more persuasive and engaging in any job field. Successful graduates of this course will be able to communicate more confidently by implementing these communication skills in both their professional and personal lives.

Course Name: Cyber Security Fundamentals for Executives

Course Number: DS-07

Clock Hours: 15

Description: The Cyber Security Fundamentals for Executives seminar provides an overview of what business executives need to know about cyber security in the context of modern technology. Through lectures, demonstrations, and discussions, students will gain a foundational perspective on the challenges of designing a cyber security program, implementing secure systems, and other factors that must be considered as part of a comprehensive cyber security solution. Topics defined include data analysis, cyber threats and defense strategies, security design principles, information assurance fundamentals, cryptography, IT systems components, networking concepts, system administration basics, and an overview of policy, IT law, ethics, and compliance.

Course Name: Computer Skills

Course Number: BC-10

Clock Hours: 15

Description: The Computer Skills seminar provides basic IT literacy and computer skills training for students with limited IT experience. The topics presented focus on skill development related to basic computer operations and information technology. Subjects include the basic concepts and techniques of computing, common personal computing hardware, Microsoft applications, typing techniques, and internet fundamentals, then continues into functions such as data input and formatting. Successful students will be able to implement this knowledge into business applications and practical real-life scenarios.

Course Name: Finance for Non-Finance Managers

Course Number: BC-11

Clock Hours: 15

Description: The Finance for Non-Finance Managers seminar provides training on key financial business principles, applying them in a real-world context for business managers without a background in finance. Throughout the course, students will work through modules that begin with understanding basic financial principles and build to applying financial analysis and ratios that drive business decision-making.

Course Name: Big Deal Closer

Course Number: BC-14

Clock Hours: 15

Description: The Big Deal Closer seminar is designed for business professionals who are seeking strategies, tips, and resources that make achieving lofty goals more attainable. Students will be trained in strategies that help improve focus and motivation while providing proven business methods for achieving exceptional results in generating new business. Successful graduates will not only be able to identify common mistakes in sales, they will understand deal-closing

strategies, how to shorten sales cycles, strategies for setting and exceeding business expectations, and price negotiation tactics.

Course Name: Entrepreneurship and Internship

Course Number: BC-20

Clock Hours: 15

Description: The Entrepreneurship and Internship seminar provides students the opportunity to learn and experience entrepreneurship first-hand, either building upon a student's current entrepreneurial venture or in planning for a startup. Students are provided with experiential learning in entrepreneurial work environments that may help them with employment opportunities in new ventures or provide knowledge—and assist with building the confidence needed—to start their own company. Students will learn how to apply entrepreneurship and business concepts to new business startups.

Course Name: Innovation Management

Course Number: BC-21

Clock Hours: 15

Description: The Innovation Management seminar provides an overview of this unique sub-discipline of management that encompasses creating, planning and supervising new organizational trends to support business growth. Topics covered include discovering new business niches, imagining new services and technologies, testing breakthrough corporate practices, establishing brand extensions, and foreseeing market trends. Students will apply innovative strategies to business intelligence and analytics, quality management, project management, marketing, IT, human resources and sales. Successful graduates will be able to complete general diffusion of innovation as problem-solving, introduce probabilities to understand how and why certain decisions lead to some outcomes instead of others, and know how to make better decisions.

Course Name: Creative Thinking

Course Number: BC-22

Clock Hours: 15

Description: The Creative Thinking seminar provides students with the essential skills needed to be able to think creatively and innovatively. Students will learn methods for reflecting in fast-paced environments, how to assimilate large amounts of information, how to communicate new ideas innovatively and engagingly, strategies for approaching problems from new angles, and how to develop novel solutions to work and industry challenges. Graduates of this course will be able to implement these methods and strategies into both their professional and personal lives.

Course Name: Digital Marketing

Course Number: BC-23

Clock Hours: 15

Description: The Digital Marketing seminar equips learners with the key foundational concepts and practical skills to begin building a marketing career in the digital age. Successful graduates of this course will understand what it takes to create and sustain a brand, conduct digital marketing through channels such as social media, analyze consumer behavior across buying contexts, understand analyze marketing metrics, along with the importance of having strategies for digital brand engagement and reputation management in today's fast-paced global economy.

Course Name: Design Thinking for Innovation

Course Number: BC-25

Clock Hours: 15

Description: In the Design Thinking for Innovation seminar, former Medtronic Chair & CEO, Professor Bill George, teaches students how to become *innovation leaders*. Students learn the essential elements of self-knowledge and identifying unique leadership gifts, motivation, and the purpose of leadership. Professor George also teaches through example, by sharing personal stories of other cutting-edge industry pioneers. Through presentation of concepts, exercises, tools, and practical tips, students are provided with a road map for becoming innovation leaders in their respective industries.