PROPOSAL FOR:

__X__NEW INSTRUCTIONAL PROGRAM

_____ SUBSTANTIAL EXPANSION/MAJOR MODIFICATION

_____ COOPERATIVE DEGREE PROGRAM

__X__WITHIN EXISTING RESOURCES or___REQUIRING NEW RESOURCES

CAPITOL TECHNOLOGY UNIVERSITY

1927

Institution Submitting Proposal

Fall 2018

Projected Implementation Date

TMBA

Award to be Offered

Technical Master of Business Administration in Cybersecurity

Title of Proposed Program

_____

Suggested HEGIS Code

11.1003

Suggested CIP Code

Business and Information Sciences

Department of Proposed Program

Dr. Helen Barker

VP Academic Affairs, CAO

Dr. Helen Barker

Contact Name

hgbarker@captechu.edu

Contact E-Mail Address

240-965-2510

Contact Phone Number

8-24-17

Signature and Date

President/Chief Executive Approval

_____

Date

Date Endorsed/Approved by Governing Board

Proposed Technical Master of Business Administration in Cybersecurity
Department of Business and Information Sciences
Capitol Technology University
Laurel, Maryland

A. Centrality to institutional mission statement and planning priorities:

1. Program description and relationship to university mission and how it relates to the institution's approved mission.

Technical Master of Business Administration in Cybersecurity Program Description:

The Technical Master of Business Administration (TMBA) in Cybersecurity provides the student with the ability to integrate business and decision-making skills in a technologically complex business environment. Capitol Technology University graduates will be able to apply their skills and knowledge of the business world to the everyday work situations in the general business environment and cybersecurity. While studying business and cybersecurity at the graduate level, the student will learn how for-profit and non-profit organizations function effectively and efficiently. Students will develop a clear picture of how business areas meld to create a successful organization. The required courses will build a solid foundation that encompasses technology, management, marketing, accounting, finance, Information Technology and human resource management.

The TMBA in Cybersecurity will prepare the student to become a metrics-driven leader in the business intelligence field. The student will learn to analyze patterns, employ powerful technological tools, and to drive business decisions in the cybersecurity field. The student will get hands-on use of the technology in business and cybersecurity.

The TMBA in Cybersecurity will prepare students to seek a career in a variety of fields, including commercial business, government, Information Technology, marketing research, sales, investment banking and more.

Relationship to Institutional Approved Mission:

The TMBA in Business is consistent with the University mission to educate individuals for professional opportunities in engineering, computer science, information technology, and business. We provide relevant learning experiences that lead to success in evolving global community. Fundamental to the degree programs in the Department of Business and Information Sciences are opportunities to integrate technology and business. The TMBA in Cybersecurity is consistent with that philosophy. This same philosophy is supported by existing degree programs and learning opportunities. The university has a D.Sc. in Cyber and a BS in Cyber and Information Security. This degree is an integral part of the strategic plan for FY 2017-2025 and forward. Funding to support the new degree has been included in institutional and departmental budgets for FY 2019-2020 and forecasted budgets going forward.

The degree will be offered online (currently using Adobe Connect and the LMS Canvas). In addition, the curriculum is supported by the same virtual labs as our current degrees in these areas. This results in the convenience required by the 21st century learner, and provides the potential for interaction with faculty and fellow students critical to the high-level learning

experience. The curriculum provides students real-world opportunities through labs and case studies, thereby providing the student the necessary practical experience the University believes critical to success in the modern business and government environments. The degree is consistent with the interdisciplinary nature of the University as well as the field of management science.

2. **Explain how the proposed program supports the institution's strategic goals and provide evidence that affirms it is an institutional priority.**

Capitol Technology University operates on five strategic goals:

1. **Elevate Education and Academic Quality:** *The University is an institution that offers career relevant curriculum with quality learning outcomes.*
2. **Expand Enrollment and Reputation:** *The University will become more globally renowned and locally active through student, faculty, and staff activities.*
3. **Diversify and Increase Financial Resources**: *The University will enhance its financial resources by expanding the range and amount of funding available to the institution, aligning costs with strategic initiatives, and expanding corporate relationships.*
4. **Maintain Institutional Viability**: *The University is committed to providing relevant learning in a quality learning environment.*
5. **Extend Our Family of Organizational Partners**: *The mission of Capitol Technology University is to provide relevant learning experiences that lead to success in the evolving global community.*

The new TMBA in Cybersecurity supports all the university's strategic goals. This approach builds upon the already successful graduate areas of study, such as the Master of Business Administration, Master of Science in Cyber and Information Security degrees, and Master of Science in Information Systems Management (which integrates business and cyber security at the graduate level). Capitol Technology University's programs are structured to teach students critical leadership, business and technical skills necessary to meet the needs of a modern technology-dependent society. The university's programs have been preparing professionals for rapid advances in technology, intense global competition, and increasingly complex technological environments for decades. The TMBA in Cybersecurity will allow students to move their skills and careers to the next level within the evolving global technological business community.

The new TMBA in Cybersecurity is fully supported by the university's Vision 2025 and Strategic Plan 2017-2021. Funding to support the degree has been included in forecasted budgets going forward.

The university has active partnerships (e.g., Leidos, Patton Electronics, Lockheed Martin, Northrup Grumman, and Cyber Security Forum Initiative, IRS, SAS) at the private and public level. The TMBA in Cybersecurity will provide new opportunities for partnerships as well as research. Potential partnerships for internships were identified at the most recent job fair held at the University. The increase in partnerships and placement of our interns and graduates in our partner institutions will serve to expand enrollment and reputation. While additional enrollment

will increase financial resources, additional partnerships and grants in this field of study will help diversify and increase financial resources.

With more and more companies relying on the security of corporate information assets and the shortage of current and potential future leaders with the necessary business knowledge in cybersecurity colleges and universities are being asked to step up to train the new workforce. Graduates with the TMBA in Cybersecurity will help fill this need, making the degree extremely relevant now and in the future.

B. Critical and compelling regional or statewide need as identified in the State Plan:

1. Demonstrate demand and need for the program in terms of meeting present and future needs of the region and the state in general based on one or more of the following:

a. The need for advancement and evolution of knowledge.

The following speaks to the increasing need of business leaders with cybersecurity knowledge:

Organizations today depend and thrive on timely, accurate and strategically relevant information. But as technology enables the creation and capture of ever-increasing amounts of data, the effective management and security of that information are becoming enormous challenges.

b. Societal needs, including expanding educational opportunities and choices for minorities and educationally disadvantaged students at institutions of higher education.

The need for highly trained cybersecurity professionals is growing at a significant rate, but the supply of cybersecurity professionals is not keeping up with the demand. According to a Burning Glass Technologies report, "Job Market Intelligence: Cybersecurity Jobs, 2015," the societal needs have not been met:

Cybersecurity jobs are in demand and growing across the economy
The Professional Services, Finance, and Manufacturing/Defense sectors have the highest demand for cybersecurity jobs.
The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%). Within these sectors, demand for cybersecurity professionals is growing rapidly in more specific industry subsectors not typically associated with cybersecurity, including Air Transportation (+221%) and Accommodation (+157%).

Positions calling for financial skills or a security clearance are even harder to fill than other cybersecurity jobs
The hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of these "hybrid jobs."

More than 10% of cybersecurity job postings advertise a security clearance requirement. These jobs, on average, take 10% longer to fill than cybersecurity jobs without a security clearance.

Cybersecurity positions are more likely to require certifications than other IT jobs
One third (35%) of cybersecurity jobs call for an industry certification, compared to 23% of IT jobs overall.

Cybersecurity employers demand a highly educated, highly experienced workforce
Some 84% of cybersecurity postings specify at least a bachelor's degree, and 83% require at least three years of experience. Because of the high education and experience requirements for these roles, skills gaps cannot easily be resolved though short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

Geographically, cybersecurity jobs are concentrated in government and defense hubs, but are growing most quickly in secondary markets
On a per capita basis, the leading states are Washington D.C., Virginia, Maryland, and Colorado; all have high concentrations of jobs in the federal government and related contractors.

Cybersecurity jobs require significant education and experience.
Some 84% of cybersecurity postings specify at least a bachelor's degree, and just as many (83%) require at least 3 years of experience, with an average of 5.4 years.

High education and experience requirements make skills gaps hard to close. Because cybersecurity jobs require years of training and relevant experience, skills gaps cannot easily be resolved though short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

The importance of properly trained cybersecurity leaders has a focus of the higher education and industry company called businessbecause.com. In a 2015 article, businessbecause.com points out that "…line between technologists and executive boards becomes increasingly blurred." The company also cited the observation by Boston Consulting Group that "[t]here is a shortage of cybersecurity professionals…and these skills are now in demand among managers and executives."

c. The need to strengthen and expand the capacity of historically black institutions to provide high quality and unique educational programs.

The industry watchdog Diverse: Issues In Higher Education serves as a source of critical news, information and insightful commentary on the full range of issues concerning diversity in American higher education. The group's recent article on August 13, 2017, "Expert: Diversifying Cybersecurity Starts with 'Targeted Recruiting,'" cites recent U.S. Bureau of Labor Statistics information regarding the high paying jobs in cybersecurity. "Yet, women and minorities are not accessing these jobs at anywhere near a proportionate rate. For instance, a report from the Business-Higher Education Forum notes that African Americans

and Hispanics represent just 6 and 7 percent of STEM employment, even though they represent more than twice that much of the U.S. population."

2. **Provide evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education.**

The 2013-2017 Maryland State Plan for Postsecondary Education articulates six goals for postsecondary education:

1. Quality and Effectiveness
2. Access, Affordability, and Completion
3. Diversity
4. Innovation
5. Economic Growth and Vitality
6. Data Use and Distribution

Goal 1

The TMBA in Cybersecurity program, with its rigor, will produce highly qualified management and decision science based professionals for an emerging field of study and employment. The university has a proven record of quality education. In addition to regional accreditation, the International Accreditation Council for Business Education (IACBE) accredits the business degrees. The TMBA in Cybersecurity program is consistent with the IACBE criteria for the delivery of high quality business education. Faculty and staff are engaged in faculty development to remain current in their field of teaching as well as to expand knowledge across disciplines. The university has in place services and learning tools to guide students to successful degree completion. Programs such as Early Alert provide staff and faculty opportunities for early student intervention in the pathway to graduation. This applies to all students regardless of mode of course delivery. Capitol Technology University is a transfer friendly institution and participates in multiple programs for government and military credit transfer. The university has multiple transfer agreements with local institutions at all degree levels.

Goal 2

The courses for the TMBA in Cybersecurity will be offered in the online format. This provides learning opportunities for students unable or unwilling to attend an on-campus institution of higher education. The University provides a tuition structure that is competitive with its competitors. The University tuition structure does not differentiate between in-state and out-of-state students. Student services are designed to provide advising, tutoring, virtual job fair attendance, and other activities supporting student completion and employment for both on-ground and online students.

Students receive information through admissions regarding the cost to attend the university. The information is also publicly available on the university website. Admissions and financial aid identify for the student potential grants, scholarships, and state plans to reduce potential student debt. The net cost versus gross costs are identified clearly for the student. Students receive advising from financial aid prior to enrolling in classes for the first time. Admissions, student services and departmental chairs advise students as to academic readiness and degree requirements. The specific success pathway is developed for each student.

The university's tuition increases have not exceeded 3%.

The university has in place services, tutoring, and other tools to help ensure student graduation and successful job placement. The university hosts a career (job) fair twice a year. The university has an online career center available to all students covering such topics as career exploration, resume writing, job search techniques, social media management, mock interviews, and assistance interpreting job descriptions, offers, and employment packages.

The university works with its advisory boards, alumni, partners, and faculty to help ensure that the degrees offered at the university are compatible with long term career opportunities in support of the state's knowledge based economy.

Goal 3

The Capitol Technology University community is committed to creating and maintaining a mutually respectful environment that recognizes and celebrates diversity among all students, faculty, and staff. The university values human differences as an asset and works to sustain a culture that reflects the interests, contributions, and perspectives of members of diverse groups. The university delivers educational programming to meet the needs of diverse audiences. We also seek to instill those values, understanding, and skills to encourage leadership and service in a global multicultural society.

The university supports various clubs that identify with diverse groups including race, gender, military/veterans, and sexual orientation. The university has a 47% minority student population with 7% undisclosed. The university's Black/African American population is 34% of the student body. The university has military/veteran population of 22%. We have a 17% female population, which is significant given that we are a technology university.

Achievement gaps: The university provides leveling courses in support of individuals attempting a career change to a field of study not necessarily consistent with their current skills. There are situations where additional undergraduate courses best serve student needs in subject areas. The university makes these courses available.

The university engages in diversity training for its institutional population, including students. Diversity and inclusiveness are built in to the curriculum allowing graduates to operate effectively in a global environment. The university supports such things a team projects and grants across degrees. This has proven effective at supporting multiple aspects of diversity.

Goal 4

Capitol Technology University's past, present, and future is inextricably intertwined with innovation. The university has a long tradition of serving as a platform for the use of new and transformative approaches to delivering higher education. New technology and cutting-edge techniques are blended with proven strategies with the goal of enabling student success in the classroom as well as in a successful career after graduation. As a small institution, Capitol can quickly integrate new technologies into the curriculum to better prepare students for the work environment. The university designs curriculum in alliance with accreditation and regulating organizations/agencies.

The university employs online virtual simulations in a game-like environment to teach practical hands-on application of knowledge. The university is engaged with a partner creating high level virtual reality environments for some courses in the degree. This all occurs in parallel with traditional proven learning strategies. These elements of the university learning environment are purposeful and intended to improve the learning environment for both the student and faculty member. In addition, these elements are purposely designed to increase engagement, improve outcomes, and improve retention and graduation rates. The university believes that innovation is the key to successful student and faculty engagement.

Example: The university engages its students in "fusion" projects, which allows students to contribute skills in interdisciplinary projects such as those in our astronautical engineering and cyber labs where business students become project managers (to send a CubeSAT on a NASA rocket) and data analysts (to analyze rainforest data for NASA). We are recruiting partners for this potential degree for which real projects will provide students integrative learning opportunities.

The university supports transfer of a limited number of graduate level courses appropriate to the degree. The university has some agreements with articulation partners for the transfer of graduate work (e.g., National Defense University).

Goal 5

One of the overarching principles of Capitol Technology University's approach to education is to instill a zeal for life-long learning in our students, which promotes economic growth and vitality of the student. Cybersecurity inherently supports a knowledge based economy. University partnerships both current and future will provide economic growth opportunities for its students, the university, and its partners. The university's PhD in Management and Decision Sciences and the D.Sc. in Cybersecurity provide opportunities for undergraduate, masters, and doctoral students to engage in high level research partnerships. The university is committed to partnering with Maryland institutions to employ our graduates to keep the talent in the state. The university instills in students an entrepreneurial attitude preparing them to bring skills to startup businesses or start a business of their own.

Goal 6

Capitol Technology University is committed to data collection and disclosure beyond the requirements of regulations and accreditation. Data is publicly available on the university website. Assessment for the university is the responsibility of the VP of Assessment and Accreditation. Highly skilled personnel are required in a timely manner to accumulate the data, analyze the data, distribute the results, and recommend potential decisions to achieve the desired outcomes. In addition, data is evaluated by the dean, chairs, faculty, advisory boards, trustees, university executives, etc. to make the best decision possible.

C. Quantifiable & reliable evidence and documentation of market supply and demand in the region and State:

1. **Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.**

   Inside Higher Ed, a leading digital media company serving higher education, recently defined the pressing need for cybersecurity professionals with business expertise in an April 26, 2017 article, "Long-term View Needed for Cybersecurity Education":

   > The projected global demand for cybersecurity talent will climb to six million by 2019, but there will be an expected shortfall of 1.5 million professionals, according to Foote Partners, which tracks information technology jobs across all skill levels. This new intersection of business and higher education is not a nice to have—for many in corporate recruiting, it's become a need to have.
   >
   > A recent Boston Globe article cited the shortage of skilled technology workers—and in particular cybersecurity talent—as the No. 1 issue for many companies. Cyberattacks increased by 48 percent in 2014, according to the accounting and consulting firm PwC, and are expected to increase as more personal computing devices become connected to the internet. And yet, the talent isn't there to support the demands of this rapidly growing industry.

   Source: https://www.insidehighered.com/digital-learning/views/2017/04/26/cybersecurity-faces-shortage-15-million-workers

2. **Discuss and provide evidence of market surveys that clearly provide quantifiable and reliable data on the educational and training needs and the anticipated number of vacancies expected over the next 5 years.**

   Eduventures, an independent research and advisory firm, points out the severe deficiency of cybersecurity professionals in an April 25, 2017 article, "Hacking the Cybersecurity Demand Curve." Eduventures points out "...a recent analysis of job posting frequencies by Economic Modeling Specialists International (EMSI) revealed an 18% increase in cybersecurity analyst jobs since 2011, distributed among more than 31,000 companies in the U.S. alone. From 2016 to 2017, there were more than 32,000 unique U.S. job postings added each month."

   Source: http://www.eduventures.com/2017/04/hacking-cybersecurity-demand-curve/

   In an April 12, 2017 article, "The Institute: The Cybersecurity Talent Shortage Is Here, and It's a Big Threat to Companies," the IEEE Cybersecurity Initiative cites the growing shortage:

   > Cisco estimates that as many as 1 million cybersecurity openings worldwide are going unfilled. And the 2016 Corporate IT Security Risks report by global cybersecurity company Kaspersky Lab found that nearly half the 4,000 businesses surveyed about their demand for specialists in the field said they were finding it difficult to fill openings.
   >
   > The talent drought is being felt across the board. Hundreds of thousands of malware intrusions alone are attempted every day, and they're not only impacting tech companies.

Institutions with data—whether it's their own, customers' or patients'—need to be concerned about protecting their systems. Nearly 70 percent of the companies surveyed by Kaspersky Lab said they planned to hire full-time cybersecurity professionals in the coming years.

Source: https://cybersecurity.ieee.org/blog/2017/04/13/the-institute-the-cybersecurity-talent-shortage-is-here-and-its-a-big-threat-to-companies/

3. **Data showing the current and projected supply of prospective graduates.**

A survey by TEKsystems ranks workers with combined business skills (strong aptitudes for business, technology, mathematics and statistics, IT) as their highest need. Both leaders and professionals say there's a already significant shortage of workers with the skills required. TEKsystems' online survey included more than 1,500 IT leaders and 2,000 IT professionals in the U.S. and Canada. TEKsystems, part of the Allegis Group, is the largest IT staffing firm in the United States.

Source: http://www.staffingindustry.com/Research-Publications/Daily-News/Big-data-important-but-there-s-a-shortage-of-skills-survey-finds-27366#sthash.VKsfVzf2.dpuf

D. Reasonableness of program duplication:

1. **Identify similar programs in the State and/or same geographical area. Discuss similarities and differences between the proposed program and others in the same degree to be awarded.**

Hood College (HC) has a Master of Science in Cybersecurity that requires 36 credits, composed of six Required 6-credit Courses, to graduate. Johns Hopkins University (JHU) has a Master of Science in Cybersecurity in three primary tracks (i.e., Analysis, Networks, and Systems) that requires 30 credits to graduate with 9 credits in Foundation Courses and 21 credits in Elective Courses. The University of Maryland (UMD) has a Master of Engineering in Cybersecurity that requires 30 credits to graduate with 18 credits in Required Courses and 12 credits in Elective Courses. The University of Maryland University College (UMUC) has a Master of Science in Cybersecurity Management and Policy and a Master of Science in Cybersecurity Technology; both degrees require 36 credits, composed of six Required 6-credit Courses, to graduate. The University of Maryland Baltimore County (UMBC) has a Master's of Professional Studies in Cybersecurity that requires 30 credits to graduate with 18 credits in Required Courses and 12 credits in Elective Courses. The University of Maryland Eastern Shore (UMES) has a Master of Science in Cybersecurity that requires 34 credits to graduate with 12 credits in Core Courses, 21 credits in Elective Courses, and 1 credit in a seminar course.

Capitol Technology University's **Technical Master of Business Administration (TMBA) in Cybersecurity program is unique in combining technically focused Master of Business Administration courses with cybersecurity courses designed to provide technical competence for future cybersecurity leaders.** The TMBA in Cybersecurity requires 36 credits to graduate with 24 credits in a set of Core Courses and 12 credits in mandatory Concentration Courses (i.e., area of concentration courses). The closest curriculum to Capitol Technology University's program is UMUC's Master of Science in Cybersecurity Management and Policy. However, UMUC's program is geared more towards cybersecurity policy.

Capitol Technology University's program is delivered online (using the Learning Management System Canvas and Adobe Connect). The programs at HC and UMBC are offered on campus. The programs at UMUC and UMES are offered primarily online. JHU's program offers a choice of online, on campus, or a mix of online and on campus. UMD delivers its program online and in person.

2. **Provide justification for the proposed program.**

   The program is strongly aligned with the university's strategic priorities and is supported by adequate resources. The new TMBA in Cybersecurity degree will strengthen and expand upon existing graduate degree programs at the university. The degree will represent study in a rapidly changing and expanding discipline. Research shows a current and growing shortage of managers and leaders grounded in cybersecurity. There is a growing shortage of individuals with the necessary combined business and cybersecurity skills in the business environment. This is an interdisciplinary academic field that helps fill those gaps. There is a thorough discussion of the need in sections B and C of this document.

E. Relevance to high-demand programs at Historically Black Institutions (HBIs):

1. **Discuss the program's potential impact on the implementation or maintenance of high-demand programs at HBIs.**

   The university is not aware of any similar high-demand programs at the Maryland HBIs.

F. Relevance to the identity of Historically Black Institutions (HBIs):

1. **Discuss the program's potential impact on the uniqueness and institutional identities and missions of HBIs.**

   The university is not aware of any impact on the uniqueness and institutional identities and missions of Maryland HBIs.

G. Adequacy of curriculum design and delivery to related learning outcomes consistent with Regulation .10 of this chapter:

1. **Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements.**

   Program description, as it will appear in the catalog:

   The TMBA in Cybersecurity program is designed to meet the growing needs of today's business and government environments where cybersecurity is now a major business consideration. TMBA Cybersecurity provides a strong managerial background, where current cyber security concepts are reviewed and analyzed through real threats and real case figures. Learn to define critical information, assess the risk of a business and make recommendations on how to reduce vulnerability.

   The TMBA in Cybersecurity will prepare students to seek leadership careers in government and private industry in such fields as healthcare, finance, and banking.

Description of program requirements:

Entrance requirements: To be fully accepted into the program, students must have completed an undergraduate degree with a cumulative GPA of no less than 3.0 on a 4.0 scale. In addition, students must also meet the program-specific prerequisites for their intended program.

Additional prerequisites for the TMBA in Cybersecurity are:

Applicants who do not possess an undergraduate degree in business must complete MBA-600 (Fundamentals of Professional Management) prior to enrolling in the core business courses; however, waivers may be granted in some cases with department chair or dean approval.

Applicants who do not have an undergraduate degree in cybersecurity or related degree may be required to take IAE-500 (Intro to Information Assurance) and CS-620 (Operating Systems Principles for Information Assurance) prior to enrolling in cybersecurity core courses; however, waivers may be granted in some cases with department chair or dean approval.

Students who have not met the 3.0 undergraduate cumulative GPA requirements, or do not meet all the program specific prerequisites, are provided an opportunity to gain full acceptance. Depending on the degree program, additional information may be requested. In this case, students are provisionally admitted and limited to three courses of enrollment. To achieve full acceptance, provisional students must maintain a 3.0 cumulative GPA in their first three graduate courses. Upon doing so, students are automatically converted to full acceptance status. If a provisional student fails to achieve a minimum 3.0 cumulative GPA after completing three courses, then he or she will be academically dismissed, and will not be permitted to enroll in any further courses.

TMBA Core Courses (24 Credits)

TMBA Core Courses focus on strengthening the student's leadership skills, enhancing the student's understanding of new technologies, expanding the student's ability to use technology to solve business problems, and understanding the process of innovation. TMBA students must take all the following courses:

MBA-616 Financial and Contract Management (3 credits)

This course is an introduction to financial and contract management for technical managers. Topics include financial management accounting (including elementary accounting principles, assets, liabilities, and stockholders' equity), direct and indirect costs, revenues, profits, indices to financial position, use of financial reports, return on investment, net present value, internal rate of return, and financial management (including cash and funds flow statements). An introduction to the principles of contract formation is presented, highlighting the distinctive characteristics of contracting with the federal government as well as the team concept for effective contracting. The role of the program manager as the key team members is a prime focus. Subcontract management, competitive negotiation techniques, contract financing, and cost reimbursement are also included. Case studies supplement theoretical discussions.

MBA-626 Organizational Behavior in Technical Environment (3 credits)

Technology has created amazing new opportunities for businesses and organizations. Mobile smartphones, tablets, all-in-one desktops and sophisticated software are just some of the radical changes that have revolutionized the workplace. Although the explosive technology growth has increased productivity and advancement, it has also created changes in worker requirements, employee expectations and workplace changes. This course analyzes organizational behavior in a technical environment. Cases are analyzed to develop skills in applying theories to common managerial problems in technology driven organizations.

MBA-627 Impact of Emerging Technology on Management and Public Administration (3 credits)

This course will focus on emerging technologies that influence management and public administration. Students will learn leading edge skills to understand the technologies and innovations that are increasingly changing the business and public administration landscape. The course will put students at the forefront of new technology to produce value for their future business, employers, and customers.

MBA-631 Technical Personnel Management (3 credits)

This course reviews the problems of personnel management in a technical organization. Topics include environmental requirements for effective and innovative technical efforts, direction and motivation, leadership behavior, recruitment of technical staff, orientation and training programs, personnel placement and reassignment, assignment of work, salary administration, personnel evaluation and counseling, professional growth and promotion, technical obsolescence and retraining, equal opportunity programs, employee grievances, and handling of conflict situations. Students explore typical personnel management situations that arise in a technical organization.

MBA-636 Technology-Enabled Operations (3 credits)

This course will prepare you to contribute effectively in today's technology-enabled workplace by understanding how to leverage processes, systems, and data to create business value. We'll examine business operations in traditional companies, between firms, and in digital businesses. We will consider the perspectives and needs of both start-ups and established organizations.

MBA-646 Project Management (3 credits)

This course provides an overview of the theory and practice of managing a project in an organizational setting. Fundamentals concepts are covered to provide a solid understanding and foundation of managing each phase of the project life cycle, adhering to organizational and cost constraints, setting goals for stakeholders, and utilizing best practices to complete the project on time and within budget. Project management is examined in the realm of various technology fields.

MBA-650 Strategic Management (3 credits)

Examines the objectives, elements and framework of analysis for strategic management. Case studies will be used as the primary tool of learning and analysis. Working well with others, synthesizing information, applying sound business judgment, and communicating crisply are key skills for this class. This class should be taken as the last core class prior to the capstone project.

MBA-700 Capstone Project (3 credits)

Students complete a research project in the field of major concentration. The research is supervised by a faculty member and must be defended by the student in an oral examination. Internships under the supervision of an academic advisor are an option. This course is to be taken last or next to last as the student applies accumulated knowledge of both core and concentration classes to this effort.

TMBA Cybersecurity Concentration Courses (12 Credits)

TMBA Cybersecurity concentration provides a strong managerial background, where current cyber security concepts are reviewed and analyzed through real threats and real case studies. Learn to define critical information, assess the risk of a business and make recommendations on how to reduce vulnerability.

IAE-685 Principles of Cybersecurity (3 credits)

This class explores the overarching security architectures and vectors of information assurance from a management perspective to allow the learner to formulate the basis for sound business decisions. Students gain an appreciation for systems, networks, processes, methodologies, documentation requirements, recovery processes, certification and accreditation processes as well as "best practice" implementation, training and continuous improvement. Discussions in this course give the correct acumen of personnel security, physical security, and technical operational security as these principles relate and interface with information security principles. Defense-in-depth principles also are covered for designing proper physical security programs. At the completion of the course students should be able to manage an IA function and evaluate an organization's Contingency Planning process for adequacy.

IAE-684 Complementary Security (3 credits)

Complementary Security is best defined as taking holistic, defense-in-depth approach to designing a complete Information Security Program. In the course, students will learn how individual domains of security from the (ISC)2 CISSP Common Book of Knowledge work together to properly address cyber risks within an organization. At the end of the course, students will be able to: (a) utilize industry best practices and frameworks to design a complete and customizable Information Security Program for any organization; (b) understand how to manage the program from an executive (CISO) level; (c) and have the knowledge necessary to take the CISSP exam.

IAE-671 Legal Aspects of Cybersecurity and Information Privacy (3 credits)

This course provides an overview of the legal rights and liabilities associated with operation and use of computers and information, including the legal and regulatory compliance issues critical for chief information security officers. It discusses the key statutes, regulations, treaties, and court cases (in the United States and abroad) that establish legal rights and responsibilities as to computer security and information privacy. The course also helps students to learn how to reduce their risk of potential legal liability for computer security or information privacy failures, and

how to enforce their security and privacy rights against other parties. Case studies and lessons learned from information security failures are used throughout the course.

IAE-674 Security Risk Management (3 credits)

This course begins with an understanding of why risk management evaluations are useful. The general methodologies for security risk assessment and security test and evaluation, including the interviews are discussed and documentation research necessary, the student is provided practical lab exercises to provide a hands-on analysis of a fictitious site. Detection, recovery, and damage control methods in contingency/disaster recovery planning research, documentation and training; methods of and procedures for contingency planning and security policy formulation and enforcement.

2. Describe the educational objectives and intended student learning outcomes.

Educational Objectives:

a. Prepare students to critically analyze problems in a variety of disciplines and to identify relevant and useful information to support the attainment of desired outcomes.
b. Prepare students to think critically by drawing appropriate conclusions from examining the output of methodological applications in the business environment.
c. Prepare students to conceptualize, apply and integrate effective strategies and to use information effectively in the decision-making process.
d. Prepare students to evaluate cyber in the context of data quality, and security and privacy regulations to determine their potential impact on information resources.

Learning Outcomes:

Upon graduation:

a. Graduates will be able to demonstrate an understanding of the legal and ethical principles applicable to the business and demonstrate the ability to apply these principles in the leadership decision-making process.
b. Graduates will be able to demonstrate a mastery of traditional and technological techniques of communicating ideas effectively and persuasively.
c. Graduates will be able to demonstrate and apply in-depth knowledge as it relates to the TMBA Technical Core Courses.
d. Graduates will be able to demonstrate an understanding and evaluate possible economic, social, legal, ethical, and environmental impacts of their business solutions.
e. Graduates will be prepared to enter global organizations with a strong understanding of business development concepts, project management processes, and team management skills.
f. Graduates will be able to develop and implement strategic management and action plans for an organization.
g. Graduates will demonstrate a strong understanding of cyber and information security concepts, project management process and team management skills
h. Graduates demonstrate familiarity with security operations and administration, demonstrate a working knowledge of infrastructure and operational security, know how to select and deploy access controls, conduct security analysis and monitoring, and apply principles of risk, response and recovery.

3. **Discuss how general education requirements will be met, if applicable.**

   N/A

4. **Identify any specialized accreditation or graduate certification requirements for this program and its students.**

   The program will be accredited regionally by Middle States, International Accreditation Council for Business Education (IACBE), with the cybersecurity courses recognized by NSA/DHS under our cyber degree recognition. Capitol Technology University is currently accredited by all three.

5. **If contracting with another institution or non-collegiate organization, provide a copy of the written contract.**

   The university will not be contracting with another institution of non-collegiate organization.

H. Adequacy of articulation:

1. **If applicable, discuss how the program supports articulation with programs at partner institutions.**

   This program does not have articulation partners currently. However, it is expected that articulation will work as it does for the university's current degrees. The university is very active with its transfer partners throughout the state and beyond. The goal of the university is to work with partners to make transfer as seamless as possible and to maximize transfer credits as allowable. There is a dedicated transfer student admissions associate to guide this process.

I. Adequacy of faculty resources (as outlined in COMAR 13B.02.03.11):

1. **Provide a brief narrative demonstrating the quality of the program faculty. Include a summary list of faculty with appointment type, terminal degree title and field, academic title/rank, status (full-time, part-time, adjunct) and the course(s) each faculty member will teach.**

   All faculty listed below have been engaged with the university for at least several years. Barker, and Pittman are fulltime faculty members. Sixteen of the twenty faculty hold terminal degrees. Cayot, Craig, Felscher, and Pullen work in the fields associated with cybersecurity. The university leadership is confident in the quality of the faculty and their abilities to provide a learning environment supportive of the goals of the university for student success. Additional doctorally-qualified faculty will be added as needed.

Instructors who will be engaged with the Technical Master of Business Administration in Cybersecurity are:

INSTRUCTOR	BACKGROUND	COURSES ALIGNED TO BE TAUGHT
Ms. Vicki Allums Adjunct	J.D. M.P.A. Comparative and International Affairs	IAE-671

	B.A.	
Dr. Audrey Andrews Adjunct	D.M. Organizational Leadership M.S. Information Systems Management M.B.A.	All MBA courses
Mr. Tommy Bargsley Adjunct	M.B.A. Applied Management B.B.A. Accounting CPA CGMA	MBA 616, MBA 650
Dr. Helen Barker Full-time	D.M. Organizational Leadership M.S. Information Systems Management M.S. Business Administration	All MBA courses
Dr. Malcolm Beckett Adjunct	D.B.A. Quality Systems Management in Homeland Security and Defense M.S. Information Systems Management	MBA 626, MBA 636
Ms. Kristen Broz Adjunct	J.D. B.A. History and English	IAE 671
Dr. William Butler Full-time	D.Sc. Cyber Security M.S. Strategic Studies B.S. Computer Science NSTISSI No. 4011 CNSSI No. 4012 NSTISSI No. 4015 CNSSI No. 4016	All Cybersecurity courses
Dr. Jami Carroll Adjunct	D.Sc. Cyber Security M.S. Cyber Security M.B.A.	All MBA courses All Cyber courses
Mr. Charles Cayot Adjunct	M.S. Information Systems Engineering B.S.	IAE 674, IAE 684, IAE 685
Mr. Jerry Craig Adjunct	M.A. Economics and Business Management M.S. Network Security & Information Assurance B.S. Computer Science PMP CISSP CCNP CCNA	IAE 685
Dr. Emily Darraj Adjunct	D.Sc. Cybersecurity M.S. Information Assurance	All MBA courses
Mr. Jack Felsher Adjunct	M.A.S. Aerospace/Aviation Management/Aviation Operations B.S.	MBA 646
Dr. George Hoffman Adjunct	D.B.A. Business Administration M.S. Systems Management B.S. Engineering Technology	All MBA courses
Dr. Priscilla Lewis Adjunct	D.M. Leadership M.B.A M.P.S Managerial Policy B.S. Economics/Mathematics	All MBA courses
Dr. Brian McElyea Adjunct	Ph.D. Leadership and Organizational Change; Specialization: Knowledge Management	All MBA courses
Dr. Alexander Perry Adjunct	D.Sc. Cyber Security M.S. Computational Mathematics	All Cybersecurity courses

Dr. Jason Pittman Full-time	Ph.D. Information Assurance M.S. Network Security B.S. English Literature and Micro-Biology	All Cybersecurity courses
Dr. Gale Pomper Adjunct	D.Sc. Cyber Security M.S. Network Security	All Cybersecurity courses
Mr. Jeffrey Pullen Adjunct	M.B.A. Project Management M.S. Public Administration M.S. Accounting B.S. Business Management FAC-P/PM, Senior Level FAC-COR, Level III PMP	MBA 616, MBA 650
Dr. Howard Van Horn Adjunct	Ph.D. Technology Management M.S. Business Administration M.S. Network Security M.S. Information Assurance PMP B.S. Special Studies Sciences	All Cybersecurity courses, MBA 627, MBA 646

J. Adequacy of library resources (as outlined in COMAR 13B.02.03.12):

1. **Describe the library resources available and/or the measures to be taken to ensure resources are adequate to support the proposed program. If the program is to be implemented within institutional resources, include a supportive statement by the President for library resources to meet the program's needs.**

   Library Services: The Puente Library offers extensive services and a wide collection for Capitol students to be academically successful. Library resources are available digitally. The library also provides a mailing service for materials borrowed through the Maryland system. The library is currently supporting a D.Sc. in Cybersecurity and PhD in Management and Business Analytics. Therefore, the library is fully prepared to support a TMBA in Cybersecurity.

   Services provided to on line students include:

   - "Ask the Librarian"
   - Research Guides
   - Tutorials
   - Videos
   - Online borrowing

   Capitol Technology University's online library as well as the on-campus library provides faculty and students with reference documents as well as texts appropriate to their learning experiences. Information about those services may be found at: https://www.captechu.edu/current-students/undergraduate/library.

   The John G. and Beverley A. Puente Library provides access to management, decision science, and research methods materials through its 10,000-title book collection, e-books, and its 90 journal subscriptions. The library will continue to purchase new and additional materials in the management, decision science, and research methods area to maintain a strong and current collection in this subject area. Students can also access materials through the library's

participation in the Maryland Digital Library Program (MDL). This online electronic service provides access to numerous databases (Access Science, NetLibrary) that will provide access to the materials needed. Available databases include ProQuest, EBSCO, ACM, Lexis Nexis, Taylor Francis, and Sage Publications.

The Puente Library can provide access to historical management and decision science materials through its membership in the Maryland Independent College and University Association (MICUA) and the American Society of Engineering Education (ASEE). Reciprocal loan agreements with fellow members of these organizations provide the library access to numerous research facilities that house and maintain archives of management and data science documents. The proximity of the University of Maryland, College Park and other local area research and academic libraries provides the Puente Library with quick access to these materials as well.

The library currently supports the needs of MBA students and cybersecurity students at the masters and doctoral level.

K. Adequacy of physical facilities, infrastructure and instructional equipment (as outlined in COMAR 13B.02.03.13):

1. **Provide an assurance that the physical facilities, infrastructure and instruction equipment are adequate to initiate the program, particularly as related to spaces for classrooms, staff and faculty offices, and laboratories for studies in the technologies and sciences. If the program is to be implemented within existing institutional resources, include a supportive statement by the President regarding adequate equipment and facilities to meet the program's needs.**

   No new facilities are required for the program. The university has sufficient classrooms to accommodate any hybrid or traditional classroom courses. The online class platform is web based and requires no additional equipment for the institution. The current learning management system meets the needs of the degree program. The Business and Technology lab and the Cyber Lab together meet the potential research needs of the students providing local and virtual support.

L. Adequacy of financial resources with documentation (as outlined in COMAR 13B.02.03.14):

1. **Complete Table 1: Resources. Finance data for the first five years of the program implementation are to be entered. Figures should be presented for five years and then totaled by category for each year.**

TABLE 1: RESOURCES

Resource Categories	Year 1	Year 2	Year3	Year 4	Year 5
1. Reallocation Funds	$25,000	$0	$0	$0	$0
2. Tuition/Fee Revenue (c + g)	$201,825	$551,333	$819,227	$1,025989	$1,224,666
a. Number of F/T Students	0	0	0	0	0
b. Annual tuition/Fee rate	$0	$0	$0	$0	$0
c. Total F/T Revenue (a x b)	$0	$0	$0	$0	$0
d. Number of P/T Students	23	61	88	107	124
e. Credit Hour Rate	$585	$603	$621	$639	$658
f. Annual Credit Hour	15	15	15	15	15
g. Total P/T Revenue (d x e x f)	$201,825	$551,333	$819,227	$1,025,989	$1,224,466
3. Grants, Contracts and Other External Sources	0	0	0	0	0
4.Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	$226,826	$551,333	$819,227	$1,025,988	$1,224,667

This proposal builds upon an existing degree programs. All courses exist within the other master's degree programs currently offered by the university.

2. **Provide a narrative rationale for each of the resource categories. If resources have been or will be reallocated to support the proposed program, briefly discuss those funds.**

a. Reallocated Funds

Capitol Technology University has reallocated funds during Year 1 for support of program and course development, online support, office materials, travel, professional development, and initial marketing. There is no substantial impact on the institution because of the reallocation of these funds. The reallocated funds will be recovered after the first year. The program is expected to be self-sustaining post Year 1.

b. Tuition and Fee Revenue

Tuition is calculated to include an annual 2.5% tuition increase. A 20% attrition rate has been calculated.

c. Grants

There are currently no grants etc. at this time.

d. Other Sources of Funds

There are currently no other sources of funds.

3. **Table 2: Expenditure. Finance data for the first five years of the program implementation are to be entered. Figures should be presented for five years and then totaled by category for each year.**

TABLE 2: EXPENDITURES
Courses are taught by adjunct professors.

Expenditure Category	Year 1	Year2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	$38,115	$117,775	$148,266	$152,714	$157,295
a. #FTE	2.3	6.8	8.3	8.3	8.3
b. Total Salary	$31,500	$97,335	$122,534	$126,210	$129,996
c. Total Benefits (20% of salaries)	$6,615	$4,798	$25,732	$26,504	$27,299
2. Admin Staff (b + c below)	$4,658	$4,798	$4,942	$5,090	$5,243
a. #FTE	.07	.07	.07	.07	.07
b. Total Salary	$3,850	$3,966	$4,084	$4,207	$4,333
c. Total Benefits	$809	$833	$858	$883	$910
3. Support Staff (b + c below)	$31,014	$84,723	$125,891	$157,664	$188,194
a. #FTE	.54	1.47	2.19	2.74	3.27
b. Total Salary	$25,632	$70,019	$104,042	$130,301	$155,533
c. Total Benefits	$5,383	$14,704	$21,849	$27,363	$32,662
4. Equipment	$920	$2,440	$3,520	$4,280	$4,960
5. Library	$0	$0	$0	$0	$0
6. New or renovated Space	$0	$0	$0	$0	$0
7.Other Expenses	$40,183	$75,133	$101,923	$122,599	$142,467
TOTAL (ADD 1-7)	$114,890	$284,869	$384,542	$442,347	$498,156

4. **Provide a narrative rationale for each of the resource categories. If resources have been or will be reallocated to support the proposed program, briefly discuss those funds.**

a. Faculty

Table 2 reflects the faculty hours in total, but this does not imply that these are new hire requirements.

b. Administrative Staff

Capitol Technology University will continue with current the administrative staff through the proposed period of time.

c. Support Staff

Capitol with continue with current administrative staff through year two. Additional support staff will be added in year 3.

d. Equipment

Software for courses is available free to students or is freeware. Additional licenses for the LMS will be purchased by the university at the rate of $40 per student. No additional equipment is needed.

e. Library

Money has been allocated for additional materials to be added to the on campus and virtual libraries to ensure currency of literature. It has, however, been determined that the current material serves the needs of this degree due to the extensive online database.

6. New or Renovated Space

No new or renovated space is needed.

7. Other Expenses

Funds have been allocated for office materials, travel, professional development, course development, initial marketing, additional scholarships.

M. Adequacy of provisions for evaluation of program (as outlined in COMAR 13B.02.03.15):

The assessment process at the university consists of a series of events throughout the Academic Year. The results of each event are gathered by the University Assessment Team and stored in Canvas for analysis and use in annual reports, assessments, etc. The University Assessment Team analyzes the results, develops any necessary action plans, and monitors implementation of the action plans.

Academic Year Assessment Events:

Fall Semester:

- Faculty submit performance plans consistent with the mission and goals of the university and department. The document is reviewed and approved with the academic dean.
- Department Chairs and University Academic Dean review the Graduating Student Survey data.
- Department Chairs and University Academic Dean review student internship evaluations.
- Department Chairs and University Academic Dean review grade distribution reports from the spring and summer semesters.
- Department Chairs and University Academic Dean review student course evaluations from the summer semester.
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations. The Advisory Board meets to begin curriculum review or address special

issues that may arise related to curriculum. Based on an analysis and evaluation of the results, the University Academic Dean, faculty and the advisory boards will develop the most effective strategy to move the changes forward.

NOTE: A complete curriculum review for degrees in the Department of Business and Information Sciences occurs every 2 years. In most cases, the changes only require that the University Academic Dean inform the CAO and provide a report that includes a justification and the impact of the changes as well as a strategic plan. Significant changes normally require the approval of the CAO and the Executive Council.

- University Academic Dean and Vice President for Academic Affairs attend the Student Town Hall and review student feedback with department chairs.
- Post-residency, the University Academic Dean meets with the faculty to review the student learning progress and discuss needed changes.
- At the August Faculty Retreat, the faculty reviews any outstanding student learning challenges that have not been addressed. The issues are brought to the University Academic Dean for review and development of implementation plans.

Spring Semester:

- Faculty Performance Plans are reviewed with faculty to identify issues of divergence and to adjust the plan as needed.
- Department Chairs and University Academic Dean review grade distribution reports from the fall semester.
- Department Chairs and University Academic Dean review the Graduating Student Survey data.
- Department Chairs and University Academic Dean review student course evaluations from the fall semester and the spring semester (in May before the summer semester begins).
- Department Chairs and University Academic Dean meet to review the content of the graduating student, alumni, and course surveys to ensure the surveys continue to meet the university's assessment needs.
- At Annual Faculty Summit in May, the faculty review and discuss student learning challenges from the past academic year and provide recommendations to the Academic Dean for review and development of implementation plans.
- Department Chairs conduct interviews with potential employers at our Career Fair (this will move to fall and spring in 2016-2017).
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations.

Based on the foregoing inputs from faculty, students, industry representatives and Department Chairs, the University Academic Dean prepares the proposed academic budget for the upcoming year. Budget increases are tied to intended student learning improvements and key strategic initiatives.
In addition to these summative assessments, the University Academic Dean meets with the Department Chairs weekly to review current student progress. This formative assessment allows for immediate minor changes, which increase faculty effectiveness and, ultimately, student outcomes.
The Faculty Senate meets monthly during August through April. The Faculty Senate addresses issues that impact student outcomes as those issues emerge. The leadership of the Faculty Senate then provides a report on the matter to the University Academic Dean. The report may include a recommendation or a request to move forward with a committee to further examine the issue. In most cases, the changes only require the University Academic Dean to inform the CAO and provide a report that includes a justification and the impact of changes as well as a strategic plan. Significant changes normally require

the approval of the CAO and the Executive Council.

Student Learning Outcomes:

Student learning outcomes are measured using the instruments identified above as well as assigned rubrics/measures (e.g. capstone courses, competency exams/projects) dictated by the accreditation requirements of regional accreditor (Middle States) our degree specific accrediting body (IACBE, ABET). This program is designed to meet the requirements of IACBE and will be reviewed for accreditation by IACBE.

N. Consistency with the State Minority Student Achievement goals (as outlined in COMAR 13B.02.03.05 and in the State Plan for Post-Secondary Education):

Capitol Technology University is a majority/minority school. Our programs attract a diverse set of students. Special attention is provided to recruit females into the STEM and multidisciplinary programs such as the B.S. MCIT, M.S. CIT, M.S. ISM, PhD. The same attention will be given to the TMBA in Cybersecurity concentration.

O. Relationship to low productivity programs identified by the Commission:

This program is not associated with a low productivity program identified by the commission.

P. If proposing a distance education program, please provide evidence of the Principles of Good Practice (as outlined in COMAR 13B.02.03.22C):

a. Curriculum and Instruction

Some courses in this concentration will be offered online in a real-time (synchronous) classroom environment as well as in hybrid (synchronous and traditional classroom).

i. A distance education program shall be established and overseen by qualified faculty.

The Department of Business and Information Sciences, where this degree will be sponsored, is staffed by qualified teaching dean and chair, and other appropriately credentialed faculty.

Evaluation of courses/programs are done using the same process as all other programs (see section M of this document). All Capitol faculty teach in the traditional classroom environment and online. (See qualifications in section I of this document)

ii. A program's curriculum shall be coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.

Online programs/courses meet the same accreditation standards, goals, objectives, and outcomes as traditional instruction at the university. The online course development process incorporated the Quality Matters research-based set of standards for quality online course design to ensure academic rigor of the online course is comparable to the traditionally offered course. The dean, chairs, and faculty review curriculum annually. Courses are reviewed at the end of each term of course delivery. This process applies to

online and traditional courses. In addition, advisory boards are engaged in the monitoring of course quality to ensure quality standards are met regardless of the delivery platform.

iii. A program shall result in learning outcomes appropriate to the rigor and breadth of the program.

Online programs/courses meet the same accreditation standards, goal, objectives, and outcomes as traditional classroom delivery. Learning platforms are chosen to ensure high standards of the technical elements of the course. The dean monitors any course conversion from in-class to online to ensure the online course is academically equivalent to traditionally offered course and that the technology is appropriate to support the expected rigor and breadth of the programs courses.

iv. A program shall provide for appropriate real-time or delayed interaction between faculty and students.

The program courses will be delivered in a format using Adobe Connect and the LMS Canvas. This system supports both synchronous and asynchronous interaction between faculty and students. Some of these class may also be in hybrid (online real-time and traditional classroom) format.

v. Faculty members in appropriate disciplines in collaboration with other institutional personnel shall participate in the design of courses offered through a distance education program.

Currently employed faculty acts as an internal advisory board for program changes including course and program development. All faculty are selected on domain experience and program-related teaching experience.

When new faculty or outside consults are necessary for the design of courses offered our Human Resource Department initiates a rigorous search and screening process to identify appropriate faculty to design and teach online courses. Again, all faculty are selected on domain experience and program-related teaching experience.

b. Role and Mission

i. A distance education program shall be consistent with the institution's mission.

Distance education is consistent with the institution's mission. Please refer to Section A (page 2) of this proposal.

ii. Review and approval processes shall ensure the appropriateness of the technology being used to meet the program's objectives

The dean and department chairs are an integral part of the curriculum approval process. The dean, chairs and faculty are participants in any new institutional technology changes. The dean approves technologies brought into the classroom by faculty to ensure compatibility with existing technology as well as with course and institutional objectives.

c. Faculty Support

i. **An institution shall provide for training for faculty who teach with the use of technology in a distance education format, including training and learning management system and pedagogy of distance education.**

The Department of Distance Learning and the instructional technology division support the online program needs of faculty and students. These departments and the help desk provide constant and on-going support to the faculty. The Canvas portion of the program is the online learning management system. When a new faculty member is assigned to teach an on-line course, the distance learning department provides formal training for that instructor. New faculty are assigned an experienced faculty mentor to ensure a smooth transition to the online environment as well as to ensure compliance with the institution's online teaching pedagogy. The university believes this provides the highest-level learning experience for students and faculty.

ii. **Principles of best practice for teaching in a distance education format shall be developed and maintained by the faculty.**

The Distance Learning Department, in conjunction with the dean and an assigned mentor, provide on-going support and instruction on best online practices. Best practices are shared among faculty by the dean and chair as well as through formal events. There are also several texts in the library available to the faculty, which cover distance learning techniques and technology.

iii. **An institution shall provide faculty support services specifically related to teaching through a distance education format.**

As mentioned previously, the university online platforms offer several avenues to support instructors engaged in online learning. The Director of our Distance Learning Division is highly skilled and trained in faculty development. Several seminars and online tutorials are available to the faculty every year. Mentors are assigned to new faculty. Best practice sharing is facilitated through the dean and chair and through formal meetings.

d. **An Institution shall ensure that appropriate learning resources are available to students including appropriate and adequate library services and resources.**

Students can receive assistance in using online learning technology via several avenues. Student aides are available to meet with students and provide tutoring support in both subject matter and use of the technology. Tutors are available in live real-time sessions using Adobe Connect or other agreed upon tools. Pre-recorded online tutorials are also available.

In addition to faculty support, on ground and online tutoring services are available to students in a one-on-one environment.

Laboratories (on ground and virtual) are available for use by all students and are staffed by faculty and tutoring staff who provide academic support.

Library services and resources are appropriate and adequate. Please refer to section J (page 17) of this document and the attached letter from the university president, the library adequately supports the students learning needs.

e. **Students and Student Services**

i. **A distance education program shall provide students with clear, complete and timely information on the curriculum, course, and degree requirements, nature of faculty/ student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.**

Students are provided support identical to traditional on campus students as the technology is utilized by all our students. Curriculum, course and degree information are available on the university website and via e-mail and mail by request. The expectations as it pertains to the faculty/student interaction are available to students during virtual open house events, literature, website, etc. In addition, this information is part of the material distributed for each course. Students receive guidance on proper behavior/interaction in the online environment to facilitate a high-level learning experience. Computer requirements are listed on our website and are provided to students in the welcome package. Student orientation and Freshman seminar provide the students information regarding academic support services and financial aid services. In addition, students visit these services at the time of their first course (s) enrollment and during placement testing events. Students are provided a list of departmental services and contacts. Technology training begins at orientation events and continues in Freshman Seminar. Students may request special/additional training to include one-on-one training.

ii. **Enrolled students shall have reasonable and adequate access to the range of student services to support their distance education activities.**

Students have access to the same services as traditional on ground students. Some of these services are facilitated via such tools as Skype. For instance, distance students attend job fairs via Skype facilitated by an assigned campus representative.

iii. **Accepted students shall have the background, knowledge and technical skills needed to undertake a distance education program.**

Students are required to have the same skills as tradition on ground students. Training is available for students to familiarize them with the tools of the distance learning system.

iv. **Advertising, recruiting and admissions materials shall clearly and accurately represent the program and services available.**

Advertising, recruiting, and admissions materials do clearly and accurately represent the program and the services available.

f. **Commitment and Support**

i. **Policies for faculty evaluation shall include appropriate considerations of teaching and scholarly activities related to distance education programs.**

All faculty, including online faculty, are strongly encouraged to participate in at least one or two professional development opportunities to improve online teaching skills. Faculty are highly encouraged to share their experiences with fellow faculty as well as through

publications and presentations. These factors are considered in the annual goals and objectives of faculty and, therefore, are considered in evaluation of performance for promotions, etc. Scholarly activities are recognized in formal university publications. Funding in the annual budget is provided for conferences in support of scholarly activities. Faculty meetings and colloquiums provide opportunities to share best practices among faculty. This includes online faculty. In addition, all faculty are offered the opportunity to attend the annual graduation ceremony and attend the annual faculty residency training event at the expense of the university.

ii. An institution shall demonstrate a commitment to ongoing support, both financial and technical, and to continuation of a program for a period sufficient to enable students to complete a degree or certificate.

The university has made the financial commitment to the program (refer to Sections L). The university has a proven track record of supporting degree completion.

g. Evaluation and Assessment

i. An institution shall evaluate a distance education program's educational effectiveness, including assessment of student learning outcomes, student retention, student and faculty satisfaction and cost-effectiveness.

The university applies the same evaluation standards and processes to all degree programs at the institution. (Please see Section M, page 22, for an in-depth process description).

In the Deprtment of Business and Information Sciences, where this program will be sponsored, evaluations are done at the course level, student level, curriculum level, and faculty level as well as other stakeholder groups.

Assessment is based on the integration of all the above items as appropriate. Changes are developed and implemented by the faculty responsible for the courses upon approval of the dean. At the end of this cycle, an evaluation is repeated and results analyzed with the appropriate stakeholders regarding the effectiveness of the changes. This is an ongoing process. The university has a vice president and team in charge of outcomes and assessment supporting formal assessment measures.

ii. An institution shall demonstrate an evidence-based approach to best online teaching practices.

Capitol Technology University has established a course/program matrix, which requires faculty to report student outcomes and suggestions for improving student performance. The university complies with the requirements of its accrediting bodies regarding outcomes/evidenced based accreditation (Middle States, ABET, IACBE, NSA/DHS). The university is in good standing with all its accrediting bodies.

iii. An institution shall provide for assessment and documentation of student achievement of learning outcomes in a distance education program.

The assessment for distance learning classes/students is the same as for all programs at the university. Faculty provide required data on student achievement. The Learning

Management System provides data on student achievement. Proof of these assessments is available during the class and post class to the VP of Assessment and Accreditation, dean, and department chairs. On an annual basis, the information is reported to accreditation authorities such as Middle States and IACBE.