EPC PROPOSAL FORM

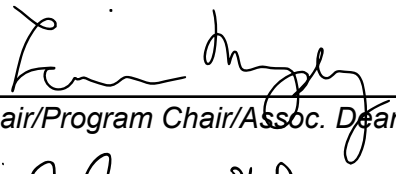
Submit **a pdf version with all appropriate signatures** (or attached email signatures with endorsement or reservations) **and a Word version** (without signatures) to facgov@plu.edu.

Deadlines: Type 3 - November 1. **Type 2** - December 1. **Type 1** - October 1 for J-Term and Spring requests; March 1 for Summer/Fall requests. *Early submission is strongly recommended.*

Originating Academic Unit(s):	Computer Science
Name of Dept. Chair/Program Chair/Assoc. Dean	Laurie Murphy
Date Proposal Submitted:	10/10/2025

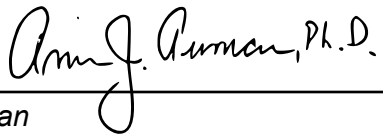
REQUIRED SIGNATURES FOR APPROVAL

(Note: Type 1 only does not require Dean or Provost signature.)



10/9/2025

*Dept. Chair/Program Chair/Assoc. Dean (**printed name and signature**)* *Date*



10/9/2025

Dean *Date*

☒ With Endorsement
☐ With Reservations

Provost *Date*

☐ With Endorsement
☐ With Reservations

PROPOSAL SUMMARY

One-sentence summary of the proposal.

Create a two year MS degree/program in Cybersecurity.

Has this proposal been formally approved by at least 2/3 of the full-time teaching faculty in your academic unit?

x Yes

☐ **No** (indicate why not)

Does this proposal impact any other academic units?

☐ **Yes** (provide email statement of support from chair of impacted units indicating at least 2/3 of the full-time teaching faculty in those units support that impact or, if not, why not)

x No

Does this proposal involve Core Curriculum elements in any way?

☐ **Yes**

x **No**

TYPE 1

Check all that apply.

☐ Add Core Curriculum element to a Special Topics course++
☐ Add, change and/or remove Core Curriculum element to an existing course++
☐ Change a course's credit hours
☐ Change course description (if change alters learning objectives or a student could retake the altered course for credit then submit as new course)
☐ Change grading type (e.g. P/F, letter grade)
☐ Catalog editorial change
☐ Change course number
☐ Change course title
☐ Prerequisite change within the academic unit only
☐ Reactivation of formerly offered course(s)

TYPE 2: SUBSTANTIVE CHANGES

Check all that apply.

☐ Add a permanent Core Curriculum course++
x Add a permanent non-Core Curriculum course
☐ Add or remove cross-listing to pre-existing course
☐ Change a concentration requirement**
☐ Change a major requirement**
☐ Change a minor requirement**
☐ Change a prerequisite involving another unit's course
☐ Create new department code
☐ Create new subject prefix
☐ Delete course
☐ Eliminate concentration
☐ Eliminate degree
☐ Eliminate major
☐ Eliminate minor
☐ Merge multiple department codes into single or new department code (indicated preferred code below)

☐ Other:

TYPE 3: NEW PROGRAMS - REQUIRES FACULTY ASSEMBLY AND BOARD OF REGENTS APPROVAL

Check all that apply.

☐ Add certificate (non-Continuing Education)^^
☐ New concentration^^
x New degree^^
☐ New major^^
☐ New minor^^
x Other:

New graduate program.

++ *Review How to Request a Core Element and then complete the Worksheet for Requesting a Core Element.*
** *Complete the EPC Curriculum Change Template and a revised two-year course cycle.*
^^ *Complete the EPC Curriculum Change Template, a revised two-year course cycle, and an Institutional Impact Evaluation Form.*

STATEMENT OF RATIONALE (1000-word limit)

Provide a statement of rationale for your requested changes. Include information on impact on student learning and outcomes.

We propose a new graduate program offering a Masters of Science in Cybersecurity. Cybersecurity is defined by the CSEC 2017 Joint Task Force on Cybersecurity Education as,

"...a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems."

This is an emerging discipline that involves the protection of people and information from adversaries. In today's highly digital and highly connected world, the safety and security of digital information has a very real impact on every citizen. Cybersecurity is vital for protecting the data and systems that support our critical infrastructure, health care systems, financial institutions, government, and most aspects of modern society. Cybercrime, ransomware, data breaches and the like have real, tangible effects on people of all backgrounds. In a very real and powerful sense, cybersecurity is about care for people.

The need for information security professionals is one of the fastest growing professions over the next 10 years. Per the Labor of Bureau Statistics, the demand for Cybersecurity professionals is expected to grow by 29% from 2024 to 2034 which represents an average of 16,000 job openings each year. The need for cybersecurity professionals spans every industry including healthcare, government, and finance.

Computer science majors have expressed an interest in cybersecurity as have prospective students at admissions events. The target population includes Bachelors' graduates with CS degrees and professionals interested in changing fields. Our proposed program seeks to meet this demand with a program that is well suited for recent graduates and professionals that are seeking to re-skill or change careers.

The list of competitors include UW, UW-T, UW-Bothell, and Seattle U. Our main competitor will be UW Tacoma as it is the only South Sound program. The main difference between these two programs is that UW Tacoma's program offers a less technical degree that has a partial focus on leadership and management, titled "Master of Cybersecurity and Leadership." It is dually taught by faculty in the Milgard School of Business and the School of Engineering and Technology. PLU's proposed program will have a more technical focus, titled "MS in Cybersecurity," will include courses such as ethical hacking and secure software development, and will be taught solely within the Computer Science department.

The modality will by hybrid/blended with regular in-person meetings during evenings or weekends. We hope that this will support working students and those with other commitments.

- **Proposed Catalog Language changes for all areas requiring change (blue Bold for additions and ~~blue Strikethrough~~ for deletions).**

The Master of Science in Cybersecurity prepares students by equipping them with the knowledge and skills necessary to address the complex challenges of protecting information systems and data. Graduates are prepared for various roles in the cybersecurity field, with a focus on the technical aspects of the discipline as well as some aspects of management and law.

Admission to the M.S. in Cybersecurity program is based on a holistic review of the applicant's academic preparation, work and volunteer experiences, and potential contributions to the classroom experience, the profession of cybersecurity, and society. Review of applications and acceptance into the program is determined by faculty evaluation. Review is based on the following requirements:

- **Bachelor's degree from an accredited institution with at least a 3.0 GPA.**
- **Knowledge of computer networking, computer programming, and mathematics. This can be demonstrated by the following:**
  - **Computer programming**
    - **Education: an introduction to programming course(s) in Java, C#, C++, C, or Python, including data structures.**
    - **Professional experience in programming**
  - **Networking**
    - **Education: an introductory computer networking course**
    - **Professional experience and/or certification in an applicable credential such as CompTIA Network+, CCNA, etc.**
  - **Mathematics**
    - **Education: courses in discrete structures and introductory statistics**

Application materials

- **Official transcript(s) from all colleges and universities attended**
- **A personal essay describing your reasons for pursuing this degree.**
- **Programming, networking and mathematics: Please describe where you acquired your knowledge of computer networking, programming and mathematics. It might be from a college course, work experience, or self-taught.**
- **A resume or vita**

Guaranteed Graduate Admission – MS in Cybersecurity

PLU's Guaranteed Graduate Admission process provides qualified students with an expedited pathway to the Master of Science in Cybersecurity.

Eligibility:
Current PLU students majoring in Computer Science (BS or BA) or Data Science (BS) with a minimum GPA of 3.0 who have completed CSCI 386, and PLU Computer Science or Data Science minors who have completed CSCI 270 and CSCI 386 and maintain a cumulative GPA of 3.0 or higher qualify for guaranteed admission.

This streamlines the admission process for high-achieving PLU students, offering a direct path from undergraduate study to the advanced Cybersecurity program.

Students who meet the eligibility requirements will receive a form that serves as their application. By completing and submitting this form, students can indicate their interest in joining the program.

Master of Science - Cybersecurity

36 semester hours

- **CSCI 501: Cybersecurity fundamentals (4)**
- **CSCI 510: Ethics, risk management, and cyber law (4)**
- **CSCI 520: Secure software development (4)**
- **CSCI 525: Network security (4)**
- **CSCI 530: Ethical hacking (4)**
- **CSCI 540: Security Operations, Incident Response and Forensics (4)**
- **CSCI 545: Cybersecurity lab (4)**
- **CSCI 550: AI and cybersecurity (4)**
- **CSCI 599: Cybersecurity capstone (4)**

Courses

CSCI 501: Cybersecurity fundamentals
A survey of the fundamental concepts, principles, and practices of cybersecurity. Designed to provide students with a comprehensive understanding of the field. Includes topics such as: basic cryptography, secure development lifecycle; common threats, vulnerabilities and exploits; confidentiality, integrity and availability; information lifecycle; privacy considerations; legal and regulatory issues. (4)

CSCI 510: Ethics, risk management and cyber law
This course explores risk management and incident response, ethics, policy and law from a cybersecurity perspective. Includes topics such as: ethics frameworks; professional ethical obligations; ethical decision making; local and federal policy; privacy; legal and regulatory issues; risk management; risk assessment and analysis; cybercrime. (4)

CSCI 520: Secure software development
This course provides an exploration of secure software development practices, emphasizing the integration of security throughout the software development lifecycle (SDLC). Students will learn to identify vulnerabilities, apply secure coding techniques, and implement security measures in software design and architecture. (4)

CSCI 525: Network security
This course explores the concepts, technologies, and methodologies used to secure networks. It covers a range of topics from fundamental principles to advanced security techniques, preparing students to design, implement, and manage secure network infrastructures. Prerequisite CSCI 501. (4)

CSCI 530: Ethical Hacking
Explores the techniques and tools used by ethical hackers to identify vulnerabilities and assess and enhance the security posture of systems and networks. Students will explore the ethical and legal implications of hacking, distinguishing between malicious hacking and ethical practices aimed at improving security. Topics include penetration testing methodologies, vulnerability assessment, and the use of various hacking tools and techniques. (4)

CSCI 540: Security Operations, Incident Response and Forensics

Students will explore the critical functions of a Security Operations Center (SOC), including threat detection, incident response, and continuous monitoring. The curriculum emphasizes the importance of establishing robust security frameworks and protocols to protect sensitive information and maintain compliance with industry regulations. Topics include the use of Security Information and Event Management (SIEM) systems, and the implementation of threat intelligence to enhance situational awareness. The topic of digital forensics is covered, where students will gain hands-on experience with forensic tools and methodologies to investigate cyber incidents. Topics such as network forensics, malware analysis, and mobile device forensics will be explored, equipping students with the skills to analyze and interpret digital evidence. Additionally, the course will cover incident response strategies, including preparation, detection, analysis, containment, eradication, and recovery. Students will learn how to develop and implement incident response plans, conduct post-incident reviews, and communicate effectively with stakeholders during and after security events. (4)

CSCI 545: Cybersecurity lab
This lab course provides students with practical experience in various aspects of cybersecurity, including network security, penetration testing, incident response, and secure coding practices. Students will engage in hands-on exercises, simulations, and projects that reinforce their understanding of cybersecurity concepts and tools. Prerequisites CSCI 525, 530, and 540. (4)

CSCI 550: AI and Cybersecurity
This course explores the intersection of artificial intelligence (AI) and cybersecurity, focusing on how AI technologies can enhance security measures and how they can also introduce new vulnerabilities. Students will gain understanding of AI applications in threat detection, incident response, and risk management as well as the ethical implications and challenges associated with these technologies. (4)

CSCI 599: Cybersecurity capstone
This can take one of two forms: internship or project. With the internship option, students secure and complete a cybersecurity-related internship, working with a faculty sponsor to set and assess learning goals. The project option involves the completion and presentation of an independent study project that makes use of the knowledge obtained from the program's curriculum to form connections between academic concepts and the application of those concepts in a real-world setting. Students present their work at the end of the program and produce a comprehensive report. (4)

If there are new courses in your proposal, please complete the following for each new course.

Course Code	Credits	Repeatable for credit?	Grade Type
CSCI 501	4	No	Standard
CSCI 510	4	No	Standard
CSCI 520	4	No	Standard
CSCI 525	4	No	Standard

CSCI 530	4	No	Standard
CSCI 540	4	No	Standard
CSCI 545	4	No	Standard
CSCI 550	4	No	Standard
CSCI 599	4	No	Standard

Does this proposal require the commitment of new or substantially different support services (e.g., Library acquisitions, Information and Technology Services, Wang Center, Internships)?

☒ **Yes** (explain what services and provide email statement of support from those areas)

The budget includes 0.5 FTE for I&TS support. This could be combined with 0.5 FTE that is anticipated to be requested for the Data Science program to make a single 1.0 FTE position that supports Computer Science, Data Science and the MS Cybersecurity program.

☐ **No**

Explain how the proposed change(s) will be staffed.

As reflected in the budget (see institutional impact form), the program will be staffed by adding 2 faculty lines over the two-year start up period. Both of the faculty will be tenure lines, one (the director) will be a 12-month appointment, and the other a 9-month appointment. The budget also reflects a 0.5 FTE for administrative staff support, and 0.5 FTE for I&TS support (see below).

If this proposal impacts regular offerings of Core Curriculum, FYEP and/or IHON courses, explain how.

N/A

Are special budgetary arrangements and funding required? If "no", explain how the proposed changes will be integrated with current financial resources. (Budgetary considerations will be reviewed/approved by Dean and Provost.)

☒ **Yes** (Explain what types of support will be used to meet the budgetary requirements of the proposed change(s). Include the source(s) of funding, percentage of costs covered, and time frame covered.)

A budget for the program was developed in consultation with the Office of Institutional Effectiveness. As reflected in the budget, the revenue generated by tuition will cover the expenses associated with new faculty lines and other costs associated with operating the program after the first year.

☐ **No**

PLU

David Wolff <wolffda@plu.edu>

MS in Cybersecurity - I&TS Support

Kevin Berg <bergka@plu.edu> Thu, Oct 2, 2025 at 8:42 AM
To: David Wolff <wolffda@plu.edu>
Cc: Ann Auman <aumanaj@plu.edu>, Laurie Murphy <murphylc@plu.edu>, "N. Justice" <justicng@plu.edu>, David Rebar <rebardm@plu.edu>, David Allen <allendp@plu.edu>

Good morning, David.
I'm writing to express support from I&TS for the MS in Cybersecurity EPC proposal that the Computer Science Department is submitting. Cybersecurity is an important field and skilled professionals are in high demand. We're excited at the prospect of having a program like this on campus and we look forward to exploring connections between the program and PLU's growing cybersecurity capabilities in I&TS.

Thank you for including us in the process and good luck with the proposal.
Kevin

--
Kevin Berg
Chief Information Officer
Information & Technology Services
Pacific Lutheran University

Institutional Impact Evaluation Form

1. **Name of Proposed Program:**

MS in Cybersecurity

2. **Executive Summary**: In 1-2 paragraphs, describe the proposed program, including a clear statement of how the program meets the mission of the university.

We propose a new graduate program offering a Masters of Science in Cybersecurity. Cybersecurity is defined by the CSEC 2017 Joint Task Force on Cybersecurity Education as,

"...a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems."

This is an emerging discipline that involves the protection of people and information from adversaries. In today's highly digital and highly connected world, the safety and security of digital information has a very real impact on every citizen. Cybersecurity is vital for protecting the data and systems that support our critical infrastructure, health care systems, financial institutions, government, and most aspects of modern society. Cybercrime, ransomware, data breaches and the like have real, tangible effects on people of all backgrounds. Cybersecurity is not just about protecting a company's "bottom line." In a very real and powerful sense, cybersecurity is about care for people.

Computer science majors have expressed an interest in cybersecurity as have prospective students at admissions events. The target population includes Bachelors' graduates with CS degrees and professionals interested in changing fields. Our proposed program seeks to meet this demand with a program that is well suited for recent graduates and professionals that are seeking to re-skill or change careers.

3. Proposed Program Start Date: Fall 2026

4. Program Offerings:

a. Describe the type of program (new degree, new major, new minor, new concentration).

New Masters of Science degree.

b. Identify the delivery format for the program (face-to-face, online, blended, or competency-based) and rationale for this format.

Classes will be delivered using a hybrid/blended format. We expect that students in this program will want greater flexibility in managing their schedules. Many will be balancing work, family, and/or other commitments. We feel that students will also appreciate the opportunity to meet in person at regular intervals. The hybrid format allows for a more flexible schedule while also giving students the benefits of in-person interaction and engagement. We expect that this will be the most attractive option for students and will also be attractive to faculty as well.

c. Describe the curriculum and program requirements by providing a clear description of the courses required to complete the program and any program-specific policies (e.g., credit hours in residency, GPA requirements). Include course offerings, number of credits, prerequisites, and any general education elements. Clearly distinguish between existing courses and any new courses that will need to be created

or deleted. If you are using preexisting catalog language, please highlight changes by using **blue boldface** for changes and ~~blue strikeout~~ for deletions.

The Master of Science in Cybersecurity prepares students by equipping them with the knowledge and skills necessary to address the complex challenges of protecting information systems and data. Graduates are prepared for various roles in the cybersecurity field, with a focus on the technical aspects of the discipline as well as some aspects of management and law.

Master of Science - Cybersecurity

36 semester hours

- **CSCI 501: Cybersecurity fundamentals (4)**
- **CSCI 510: Ethics, risk management, and cyber law (4)**
- **CSCI 520: Secure software development (4)**
- **CSCI 525: Network security (4)**
- **CSCI 530: Ethical hacking (4)**
- **CSCI 540: Security Operations, Incident Response and Forensics (4)**
- **CSCI 545: Cybersecurity lab (4)**
- **CSCI 550: AI and cybersecurity (4)**
- **CSCI 599: Cybersecurity capstone (4)**

Courses

CSCI 501: Cybersecurity fundamentals
A survey of the fundamental concepts, principles, and practices of cybersecurity. Designed to provide students with a comprehensive understanding of the field. Includes topics such as: basic cryptography, secure development lifecycle; common threats, vulnerabilities and exploits; confidentiality, integrity and availability; information lifecycle; privacy considerations; legal and regulatory issues. (4)

CSCI 510: Ethics, risk management and cyber law
This course explores risk management and incident response, ethics, policy and law from a cybersecurity perspective. Includes topics such as: ethics frameworks; professional ethical obligations; ethical decision making; local and federal policy; privacy; legal and regulatory issues; risk management; risk assessment and analysis; cybercrime. (4)

CSCI 520: Secure software development
This course provides an exploration of secure software development practices, emphasizing the integration of security throughout the software development lifecycle (SDLC). Students will learn to identify vulnerabilities, apply secure coding techniques, and implement security measures in software design and architecture. (4)

CSCI 525: Network security
This course explores the concepts, technologies, and methodologies used to secure networks. It covers a range of topics from fundamental principles to advanced security

techniques, preparing students to design, implement, and manage secure network infrastructures. Prerequisite CSCI 501. (4)

CSCI 530: Ethical Hacking
Explores the techniques and tools used by ethical hackers to identify vulnerabilities and assess and enhance the security posture of systems and networks. Students will explore the ethical and legal implications of hacking, distinguishing between malicious hacking and ethical practices aimed at improving security. Topics include penetration testing methodologies, vulnerability assessment, and the use of various hacking tools and techniques. (4)

CSCI 540: Security Operations, Incident Response and Forensics
Students will explore the critical functions of a Security Operations Center (SOC), including threat detection, incident response, and continuous monitoring. The curriculum emphasizes the importance of establishing robust security frameworks and protocols to protect sensitive information and maintain compliance with industry regulations. Topics include the use of Security Information and Event Management (SIEM) systems, and the implementation of threat intelligence to enhance situational awareness. The topic of digital forensics is covered, where students will gain hands-on experience with forensic tools and methodologies to investigate cyber incidents. Topics such as network forensics, malware analysis, and mobile device forensics will be explored, equipping students with the skills to analyze and interpret digital evidence. Additionally, the course will cover incident response strategies, including preparation, detection, analysis, containment, eradication, and recovery. Students will learn how to develop and implement incident response plans, conduct post-incident reviews, and communicate effectively with stakeholders during and after security events. (4)

CSCI 545: Cybersecurity lab
This lab course provides students with practical experience in various aspects of cybersecurity, including network security, penetration testing, incident response, and secure coding practices. Students will engage in hands-on exercises, simulations, and projects that reinforce their understanding of cybersecurity concepts and tools. Prerequisites CSCI 525, 530, and 540. (4)

CSCI 550: AI and Cybersecurity
This course explores the intersection of artificial intelligence (AI) and cybersecurity, focusing on how AI technologies can enhance security measures and how they can also introduce new vulnerabilities. Students will gain understanding of AI applications in threat detection, incident response, and risk management as well as the ethical implications and challenges associated with these technologies. (4)

CSCI 599: Cybersecurity capstone
This can take one of two forms: internship or project. With the internship option, students secure and complete a cybersecurity-related internship, working with a faculty sponsor to set and assess learning goals. The project option involves the completion and presentation of an independent study project that makes use of the knowledge obtained from the program's curriculum to form connections between academic concepts and the application of those concepts in a real-world setting. Students present their work at the end of the program and produce a comprehensive report. (4)

d. Provide a two-year course cycle for delivering the curriculum.

	Fall 2026	JTerm 2027	Spring 2027	Sum. 2027	Fall 2027	JTerm 2028	Spring 2028
CSCI 501 Cybersecurity fundamentals	x				x		
CSCI 510 Ethics, risk management and cyber law	x				x		
CSCI 520 Secure software development			x				x
CSCI 525 Network security			x				x
CSCI 530 Ethical hacking					x		
CSCI 540 Sec. Ops, incident response and forensics					x		
CSCI 545 Cybersecurity lab					x	x	
CSCI 550 AI and cybersecurity							x
CSCI 599 Cybersecurity capstone							x

e. Provide completion pathways (including two and four-year advising plans for undergraduate programs).

Year 1

Fall	**J-Term**	**Spring**
CSCI 501: Cyber. Fundamentals (4) CSCI 510: Ethics, risk, and cyber law (4)		CSCI 520: Secure SW Development(4) CSCI 525: Network security (4)

Year 2

Fall	**J-Term**	**Spring**
CSCI 530: Ethical hacking (4) CSCI 540: Security Operations, Incident Response and Forensics (4)	CSCI 545: Cybersecurity lab (4)	CSCI 550: AI and cybersecurity (4) CSCI 599: Capstone

f. Identify the learning outcomes for the program. For undergraduate programs, also describe the connection to the Integrative Learning Objectives.

Learning Outcomes

1. Demonstrate proficiency in the use of cybersecurity tools and technologies

2. Be able to analyze and implement security measures to protect network and software infrastructures from threats
3. Analyze a given cybersecurity scenario to identify potential legal and ethical conflicts, and propose a course of action that aligns with professional and societal standards.
4. Develop a personal professional development plan that outlines specific strategies for staying current with emerging cybersecurity threats and industry best practices.

g. Provide a plan for assessing program learning outcomes.

The director of the program will develop a detailed assessment plan during the second year of the program. The director will oversee the implementation of that plan on a regular basis.

h. Identify program entrance requirements, including application processes, if appropriate.

Admission to the M.S. in Cybersecurity program is based on a holistic review of the applicant's academic preparation, work and volunteer experiences, and potential contributions to the classroom experience, the profession of cybersecurity, and society. Review of applications and acceptance into the program is determined by faculty evaluation. Review is based on the following requirements:

- **Bachelor's degree from an accredited institution with at least a 3.0 GPA.**
- **Knowledge of computer networking, computer programming, and mathematics. This can be demonstrated by the following:**
  - **Computer programming**
    - **Education: an introduction to programming course(s) in Java, C#, C++, C, or Python, including data structures.**
    - **Professional experience in programming**
  - **Networking**
    - **Education: an introductory computer networking course**
    - **Professional experience and/or certification in an applicable credential such as CompTIA Network+, CCNA, etc.**
  - **Mathematics**
    - **Education: courses in discrete structures and introductory statistics**

Application materials

- **Official transcript(s) from all colleges and universities attended**
- **A personal essay describing your reasons for pursuing this degree.**
- **Programming, networking and mathematics: Please describe where you acquired your knowledge of computer networking, programming and mathematics. It might be from a college course, work experience, or self-taught.**
- **A resume or vita**

Guaranteed Graduate Admission – MS in Cybersecurity

PLU's Guaranteed Graduate Admission process provides qualified students with an expedited pathway to the Master of Science in Cybersecurity.

Eligibility:
Current PLU students majoring in Computer Science (BS or BA) or Data Science (BS)

with a minimum GPA of 3.0 who have completed CSCI 386, and PLU Computer Science or Data Science minors who have completed CSCI 270 and CSCI 386 and maintain a cumulative GPA of 3.0 or higher qualify for guaranteed admission.

This streamlines the admission process for high-achieving PLU students, offering a direct path from undergraduate study to the advanced Cybersecurity program.

Students who meet the eligibility requirements will receive a form that serves as their application. By completing and submitting this form, students can indicate their interest in joining the program.

5. **External Authorization**: Will the proposal require authorization from NWCCU, the state of Washington, or an external accreditation body?

No

6. **Rationale**:

   a. Provide evidence of demand for the proposed program, which may include a market analysis or review of trends at other universities. Include reference to relevant competitors' programs and characteristics of the proposed program that will make it attractive to students in light of this competition.

The need for information security professionals is one of the fastest growing professions over the next 10 years. Per the Labor of Bureau Statistics, the demand for Cybersecurity professionals is expected to grow by 29% from 2024 to 2034 which represents an average of 16,000 job openings each year. The need for cybersecurity professionals spans every industry including healthcare, government, and finance.

The list of competitors include UW, UW-T, UW-Bothell, and Seattle U. Our main competitor will be UW Tacoma as it is the only South Sound program. The main difference between these two programs is that UW Tacoma's program offers a less technical degree that has a partial focus on leadership and management, titled "Master of Cybersecurity and Leadership." It is dually taught by faculty in the Milgard School of Business and the School of Engineering and Technology. PLU's proposed program will have a more technical focus, titled "MS in Cybersecurity," will include courses such as cryptography and secure software development, and will be taught solely within the Computer Science department.

   b. Identify the target audience for the program.

The target audience includes recent graduates of Bachelor's programs in CS, math or closely related fields, professionals seeking to re-skill, and Bachelor's graduates from other disciplines.

   c. Explain why this is the right time for the university to add this program.

Cybersecurity is a new, emerging discipline and the need for cybersecurity professionals is growing. Prospective students are increasingly interested in the field, as evidenced by significant numbers asking about it at recruitment events. This, coupled with the fact that the PLU administration views the strengthening of its graduate programs as a way toward financial growth and stability makes this the right time.

   d. Explain how this program might compete with other programs currently offered at PLU.

We do not foresee any competition with existing graduate programs except perhaps for the MBA program. There may be some students interested in the MBA who might consider a cybersecurity degree because of the importance of cybersecurity in business. However, we do not expect this to cause a significant impact to the MBA program, which has been well enrolled for years, and this program has prerequisites that the MBA does not.

e. Identify which academic units might be affected by this program, and how.

This will not affect any academic units outside of the computer science department.

f. Will approval of this program mean the termination of another program? If so, what is the timeline for the proposed elimination?

No.

7. Marketing strategies:

a. Provide a marketing and advertising plan for the initial roll-out of the program, including a timeline.

The proposal budget includes funds allocated for marketing. If approved by faculty assembly and PLU Board of Regents, marketing would initially begin in the spring and summer of 2026. The budget also includes an administrative faculty position (director) whose duties will include recruiting and admission. Marketing will focus on three areas: (1) direct marketing to current PLU students and recent graduates from undergraduate programs; (2) recent graduates throughout the state of Washington; and (3) the local community.

Digital marketing will focus on social media advertising and search engine optimization.

The CSCI department has an Industry Advisory Board consisting primarily of alumni who work in the technology industry. We will notify them of this new program and provide them with print and digital content that can be further distributed by them.

b. Identify longer-term plans for marketing and advertising.

The budget also includes funds for marketing long-term. The program will work with the Graduate Admission Office and PLU MARCOM to develop long-term marketing strategies based on what we learn from initial marketing efforts.

8. External funding sources: Describe any plans for the development of funding sources for this program that are external to the university, including projected amounts of funding for each.

a. Fundraising: None

b. Grants: None

c. Other: None

9. Faculty, Staff and Administration:

a. Describe the qualifications needed by faculty who will teach in the program.

PhD in cybersecurity or closely related field.

b. Identify the number and type (contingent, tenure-track) of faculty members necessary to deliver the program.

Year one of the program will require one faculty member to direct the program, develop courses, and teach. In year two, one additional faculty member will be required to develop courses and teach them. Moving forward, the teaching load and director's position can be filled by two tenure-track faculty.

c. Will any current faculty serve in the proposed program? If so, how will this new commitment be accommodated in their teaching load?

No current faculty will serve in this program.

d. Identify the number and type (contingent, tenure-track) of *new* faculty necessary to deliver the program.

Two new tenure-track new faculty are necessary, with only one required during year one. The director of the program will be given a 50% administrative release time starting in year two, with 33% release in year one.

e. If new faculty are required, provide a recruitment plan and timeline, including comments addressing the challenges of filling positions with small hiring pools or where market premia might be required.

The search for the first faculty member will begin shortly after the program is approved by the PLU Board of Regents, with the goal of starting the position in the Spring or Summer of 2026. During that Spring and Summer, the person would prepare courses, administer and help market the program. The search for the second faculty member will begin in the Fall of 2026 with the position to begin in the Fall of 2027.

The hiring pool for these positions is expected to be small, so we will:

- Provide a premium salary for Assistant, Associate, and Full professors to capture the full pool of potential faculty.
- Utilize connections through CSCI alumni.
- Advertise through academic job boards, and cybersecurity specific job sites such as cybersecurityjobs.com

f. Describe plans for providing administrative support for the program. Identify any new administrative positions or organizational rearrangements in staff needed to accommodate the new program.

Administrative support for this program will fall under the College of Natural Sciences and the Department of Computer Science. As part of this new program, we have a request to add an additional 0.50 FTE to the College of Natural Sciences to support the ever-growing Computer Science programs, and a 0.5 FTE to I&TS to support both this program and the Data Science major. The latter can be combined with the 0.5 FTE that was requested as part of the Data Science proposal to make a full time I&TS position dedicated to the Computer Science, Cybersecurity and Data Science programs.

10. **Facility and Technology Needs** – Includes but not limited to classroom, office, studio, laboratory, storage, technology, and computer labs.

    a. Describe any new construction or facility renovations necessary to launch or maintain the program and the associated expenses.

Classes will be held in the Morken Center for Learning and Technology, using CSCI classroom space, which is available in the evenings and weekends. The addition of 2 new faculty members can be accommodated in existing office spaces in Morken.

    b. Describe any furniture and/or equipment necessary to launch or maintain the program.

Existing furniture will be sufficient.

The only equipment needed are the computers and servers that currently reside within the CS department. However, the Cybersecurity lab may require the purchase of online services or software that provide cybersecurity training. Funding for this is included in the budget.

    c. Explain any special security considerations associated with the program.

None

    d. Identify possible health and safety concerns associated with the program.

None

11. **Library Resources**:

    a. Describe library resources needed to support the program, including print books, electronic materials, and other library resources.

No

    b. Does the new program require access to library resources not already available? Are these mandated by any program accreditation?

No

    c. If the program is fully online or blended, describe how library resources will be delivered to students. Include expenses for postage, photocopying, etc.

N/A

12. **Student Services**—Are there any changes in existing student services needed to accommodate the program? Will adding the program result in changes in service provision to the rest of the student body? Where might additional resources be necessary, and what are the projected expenses for those resources?

    a. Financial aid

Financial aid will fall under the same awarding policy as all other graduate programs.

b. Registration

The program director will provide support to students in the program.

c. Center for Student Success (advising, tutoring)

None

d. Other

Current staff support from the Office of Admissions and Graduate programs may provide support for the program. Students may need access to buildings during evenings and weekends.

13. Budget. Use information from the questions above to complete the table. Please see footnotes for additional information.

Year	Year Zero	Academic Year 1	Academic Year 2	Academic Year 3	Academic Year 4
# Students in Program[i]		10	25	35	40
# Faculty FTE to Deliver Program[ii]	.5	2.0	2.0	2.0	2.0
# *New* Faculty FTE to Deliver Program[iii]	.5	2.0			
Average Faculty Salary in unit[iv]		114,000	117,420	120,950	124,570
# Administrators or Staff[v]			1.0	1.0	1.0
# *New* Administrators or Staff[vi]			1.0		
Average Administrator or Staff Salary[vii]			50,000	50,000	50,000
Services & Purchases[viii]	30,000	40,000	40,800	41,600	42,500
Facility and Technology[ix]					
Library Resources[x]					
Student Services[xi]					
Net	-108,000	152,720	339,970	461,920	481,185

i. Identify the projected number of students *declared* in the new program for each of the first <u>four</u> years of the program.

ii. Identify projected faculty FTE for each of the first <u>four</u> years of the program.

iii. Identify the number of additional (new) faculty FTE (whether new of contingent) necessary to add in each of the first four years of the program.

iv. Identify average faculty salary in the proposed program in consultation with the Provost's Office.

v. Indicate the projected staff/administrator FTE for each of the first four years of the program.

vi. Identify the number of additional (new) staff/administrator FTE necessary to add in each of the first four years of the program.

vii. Indicate the average staff/administrator salary.

viii. Indicate the annual services and purchases budget required for each of the first four years of the program, including any projected expenditures required for start-up expenses. *Itemize these expenses in an attached narrative*.

ix. Estimate facilities and technology expenses for each of the first four years of the program.

x. Estimate library expenses for each of the first four years of the program.

xi. Estimate student services expenses

14. **Risk management -** Describe the major risk considerations of the plan and the steps that could be taken to mitigate or minimize the risk and still implement a successful plan. For example, if applicable, the plan may encounter problems associated with items such as negotiating a lease contract, obtaining city or government approvals, obtaining accreditation approval, etc.

There is no significant risk to the program related to accreditation, however, it would be advantageous to seek a CAE (Center of Academic Excellence) designation. This designation, while valuable, is not critical to the success of the program. We intend to ask the director of the program to make this a priority during the first few years of the program.

Possibly the most significant risk is the hiring of the director for year one. It will likely be challenging to find someone qualified to shepherd and teach this program. We plan to make use of all resources available to distribute the position announcement as widely as possible. It is also important that we make the position open-rank to attract more experienced faculty and to offer a competitive salary.

15. Accountability and Exit Strategy:

a. Outline the steps that will be taken to review whether the program is meeting its enrollment and revenue targets, including the timeline for such review. For new undergraduate programs, provide a 5-year timeline; for new graduate programs, provide a 3-year timeline.

The MS in Cybersecurity will be assessed annually to measure viability in both enrollment and finances. This annual review occurs at the end of every fiscal year.

b. Provide an exit strategy, including a general timeline for deciding whether to terminate or continue the program and a plan for teaching out the program.

If after the annual review, mentioned above, the program is determined to no longer be viable the program will teach out the current students and put the application and admit process on pause for further review. Any tenure-track faculty hired for the program will be offered opportunities to teach in

related curricula (CSCI, DATA) and/or Gen Ed courses to support other university needs. Added staff support will also be evaluated to determine if there is a continued need.

c. Identify who will be responsible for providing accountability and oversight for the program meeting its enrollment and revenue targets.

The Dean of the College of Natural Sciences, the Director of the Cybersecurity program, the Dean of Admission, and the Chief Analytics Officer will all be responsible for reviewing the program.

16. Communications Checklist. The persons/offices listed below should be consulted as the proposal is prepared.

	Signature	**Date**	**Level of Support:** ● **Support** ● **Undecided** ● **Do not support**
Academic Unit Head			
College Dean			
Associate Provost for Undergraduate or Graduate Studies, as appropriate			
Accreditation Liaison Officer			
Director of the Library			
Student Financial Services			
Director of Admission for Undergraduate or Graduate, as appropriate			
Executive Director Center for Student Success			
Vice President for Administrative Services			
Director of Financial Operations			

Electronic signatures were collected via a Google Form. Responses are summarized below.

Date	Title	Name	Level of Support
10/9/2025	Chair of Computer Science Department	Laurie Murphy	I support
10/9/2025	Dean of the College of Natural Sciences	Ann Auman	I support
9/26/2025	VP of Administrative Services	Shalita Myrick	I support.
9/26/2025	Executive Director for Student Success	Kris Plaehn	I support.
9/26/2025	Dean of Admission	Melody Ferguson	I support.

9/30/2025	Dean of Enrollment Management & Student Financial Services	Mike Frechette	I support.
10/6/2025	Dean of the Library	Joe Toth	I support.
10/6/2025	Associate Vice President and Chief Institutional Effectiveness Officer	Karen McConnell	I support.

Educational Policies Committee
Curriculum Change Template

Current Courses	Current Hours	Proposed Courses	Proposed Hours
		MS Cybersecurity	**36 Hours**
		CSCI 501	4
		CSCI 510	4
		CSCI 520	4
		CSCI 525	4
		CSCI 530	4
		CSCI 540	4
		CSCI 545	4
		CSCI 550	4
		CSCI 599	4