**Appendix A – Catalog Description**

**Program Overview**

This certificate is intended to provide students with knowledge, skills and experience sufficient to develop and implement cybersecurity governance, policy and risk programs based on common frameworks.

Please note that a complementary certificate, “Cybersecurity – Technologies” explores the security of systems of computers and networks and develops the skills to implement or operate these securely. These two certificates cover most of the courses in the MS degree, however students need to take three more courses plus Semester-In-Residence project to complete their master degree. The selected courses in the certificate program are the pre-requisites of the remaining courses of the master program.

The PSM Cybersecurity students will automatically receive this certificate after successful completion of the courses required for this certificate.

**Program Students Learning Outcomes**

Upon completion of the program, students will be able to:

1. Analyze an organization’s critical information, and assets related to developing a security schema and security governance & policy framework
2. Develop management knowledge, skills, and behaviors, related to structuring team dynamics, project management, and response to change
3. Identify economic and regulatory issues related to cybersecurity operations
4. Analyze risks and operationalize security decisions to meet compliance and business objectives

**Admission Requirements and Application**

* Admission decisions will be made by the Admission Committee chosen by the Program Director in consultation with its faculty
* Admission decisions will be based on 1) undergraduate courses and GPA, 2) resume or GRE scores, and 3) TOEFL for some students \*\*
* Admission to the program requires an undergraduate degree in computer science or closely related discipline and should include upper-division courses in operating systems, networks and software engineering. Applicants with a baccalaureate degree in a related field may be able to meet prerequisites with equivalent work experiences in computer science and will be considered for conditional admission.
* Admission requires a minimum of 3.0 grade point average in the upper-division computer science courses and at least a 2.5 undergraduate GPA in the last 60 semester units (or last 90 quarter units) attempted.
* All applicants must submit general GRE scores, or resume when applying.
Minimum GRE scores required are:
- Verbal 143
- Quantitative 155
- Analytical Writing 3.5
* As an alternative to the GRE, applicants may submit a resume or CV showing work experience in Cybersecurity or technology field.

Applicants must submit:

1. The program application form.
2. GRE scores, or resume.
3. TOEFL score if required.
4. One set of transcripts from all colleges/universities attended.
* Applicants to the program will be subject to standard background checks in accordance with Defense Security Service reporting requirements.

Student candidates may apply at any time throughout the year. However, selection and admission will be completed by early May for the Fall semester start. Later applications will be considered, as spaces remain available. Feedback to applicants, but not final admission decisions, will be provided on a timely basis regardless of the time of application.

\*\*All applicants must have a TOEFL score of 80 iBT or above (213 on the computer-based examination, 550 paper-based), or an IELTS score of 6.0, unless they possess a bachelor’s degree from a post-secondary institution where English was the principal language of instruction.

**Certificate Requirements and Courses**

The Cybersecurity –Management, Risk & Governance certificate requires students to complete the following set of courses. Students must maintain a 3.0 GPA and earn at least a "C" (2.0) in each course.

**Required Courses Total: 12 units**

|  |  |
| --- | --- |
| ***MCS 500*** | ***Introduction to Cybersecurity (2)*** |
| ***MGMT 521*** | ***Principles of Organizational Behavior and Leadership for Security Management (2)*** |
| ***MIS 522*** | ***Information Systems and Security Management (2)*** |
| ***MIS 621*** | ***Information Security Governance (3)*** |
| ***MIS 622*** | ***Technology Assessment and Security Risk Management (3)*** |

Students must maintain an overall GPA of 3.0 and earn at least a C (2.0) in each course, except those taken for credit/no credit. Any student whose overall GPA falls below 3.0 for two consecutive semesters will be dropped from the program. A full-time student should be enrolled in the predetermined course schedule and credit hours each semester for the program