



CENTER OF ACADEMIC EXCELLENCE

# CYBER Operations

## Continuous Improvement Plan

The University of Arizona Continuous Improvement Plan includes four main components to enhance the overall quality of our Cyber Operations program: our Strategic Planning Process; the Program-Level Learning Outcomes; Assessments of the Program-Level Learning Outcomes; and the Proposed Program Changes. See below for the details of each component:

### Strategic Planning Process

To keep the University of Arizona Cyber Operations curriculum current and relevant, a standardized course and instructor review process is performed at the end of each academic year. This process examines the quality and relevance of course content; evaluates the effectiveness of instruction; and incorporates the results of student feedback on formal Teacher/Course evaluation surveys. Due to the rapidly evolving nature of the field of cyber operations, our faculty are committed to staying abreast of current events in cyberspace, new and innovative offensive/defensive cyber operations tactics, techniques, and tools. Each year an interdisciplinary board is assembled to examine our research results, assess current events in offensive/defensive cyber operations tactics, techniques, and tools, and analyze input from other Cyber Operations community members. These data are reviewed to identify any programmatic or individual course deficiencies and utilized to support continuous updating of course content and relevance.

### Program-Level Learning Outcomes

The University of Arizona Cyber Operations program has three main program-level learning outcomes that are used for institutional assessment and accreditation. These outcomes represent a synthesis of the main areas that are introduced, reinforced, and assessed within the Cyber Operations program. The following are the program-level learning outcomes:

1. **Critical Thinking & Problem Solving** - Demonstrate understanding of how variability affects outcomes; how to identify anomalous events; how to integrate and differentiate continuous functions of multiple variables; and how to solve complex problems using computation and scripting languages.
2. **Digital Citizenship** - Describe and explain the relationship between cyber ethics and law; criminal penalties related to unethical hacking; and apply the notion of Gray Areas to articulate where the law has not yet caught up to technology innovation.
3. **Technical Competencies & Analysis** - Demonstrate and explain an understanding required to apply specific technical principles and information in a job function or role. Demonstrate the difference between critical and irrelevant pieces of information and gather information from a variety of sources to reach a conclusion.

### **Assessments of the Program-Level Learning Outcomes**

The process of Program Assessment is conducted by the Department Head, Josh Pauli. The current backup for this process is the senior faculty member in the department, Paul Wagner. Capstone grades and exit survey results will be compiled and evaluated after the spring semester. Data will be reviewed by program director and department head prior to the fall semester. Results will be presented to faculty upon return to work during the fall semester (August) to gain input on program assessment which is due September 30.

The Cyber Operations Program Office will administer surveys to the graduates of the Cyber Operations degree program. The first survey will be administered in the CYBV 498 program capstone course and will be a required course component. A draft of this survey instrument is included and is designed to provide more general information about student opinions on the degree program's alumni support options, job placement, and preparedness to work in the Cyber Operations field.

The second survey will be emailed out by the Program Manager for Cyber Operations three months after graduation, with a telephone call reminder to complete the survey from the Cyber Operations Program Office, if necessary. It will be emailed out again nine months after graduation, with a telephone call if necessary, from the Cyber Operations Program Office. Thereafter, the survey will be administered once per year to continue to provide longitudinal data to the Program Director, faculty members, and the Advisory Board.

Further program assessment will be provided by the Advisory Board. To meet the needs for being recognized as a Center of Academic Excellence in Cyber Operations (CAE-CO), the Cyber Operations program needed to create an Advisory Board to provide input to the Program Director and faculty on changing industry needs and developments that may need to be included in the current course curriculum. The Advisory Board consists of leaders in different portions of the cyber field, including those working in the government, the military, and private sector. The Advisory Board will be convened twice each calendar year for a meeting with the current faculty members and the Program Director to review the Cyber Operations BAS curriculum to be certain it is adjusting as needed to meet market demands and to ensure that the knowledge, skills, and abilities employers are seeking are being addressed by our curriculum.

### **Proposed Program Changes**

As part of the NSA designation process, the Cyber Operations degree program is required to provide curriculum updates at least once per year to verify that the curriculum is staying current in a quickly changing field. The Cyber Operations BAS program at the University of Arizona has included a once yearly review of curriculum in their documentation to the NSA. This review includes a minor review after the end of the Fall semester, and a more stringent review at the end of the Spring semester each year. This provides the opportunity for minor revisions before a course may be taught again, and time for more major adjustments during the summer prior to courses resuming in the Fall semester.

The University of Arizona conducts continuous curriculum updates as a standard part of our process. With the impending KU changes within the CAE-CO program, the University of Arizona is not proposing any major changes to its program at this time. We will continue to

support the development of the new CAE-CO KUs then will make the appropriate changes to align our program to the new Mandatory and Optional KU Content areas.