2024 Risk Mitigation Plan Highlights Appendix

Safety and Security

Several activities related to safety and security have taken place and are planned:

- The CCCS Director of Emergency Management conducted physical security reviews at all colleges. Risk mitigation plans from physical security reviews are being updated. Details of these assessments are shared with the Board annually in Executive Session, generally in February.

- Training continues to occur at the System Office and the colleges, as appropriate, to ensure staff are prepared and trained in the event of an emergency. Training includes active shooter response, mental health first aid and bleeding control.

- To prepare for a disaster, stand-by emergency contracts, a system resource list, facility use agreements, and an emergency management finance policy are in place. Colleges continue to develop continuity of operations plans.

- A critical incident recovery planning template that provides resources for presidents and senior leadership was shared with all colleges.

Financial Aid

To reduce the risks related to financial aid, the following activities are in process:

- Advocacy for increased financial aid availability and foundation partnerships. In addition, in spring 2022, a two-year pilot program was launched and is in progress for Concurrent Enrollment students which is intended to cover costs not paid by school districts.

- Task forces and meetings continue to discuss changing financial aid regulations, best practices, and ensuring programs continue to meet requirements for financial aid. The coming years will continue to see significant changes to financial aid processes due to the FAFSA Simplification Act.

- Centralized processing at the System Office for five rural colleges and colleges with temporary shortages and staff turnover, which includes the addition of another financial aid team member. An FTE was added to allow the System Office to better support the colleges. The System Office is reviewing areas to centralize and reduce the administrative burden on colleges.

- The System continues to provide centralized training and documentation of processes. Membership to the National Association of Student Financial Aid Administrators will be purchased to provide additional training and timely updates system wide. Reports to detect potentially fraudulent student financial aid applications are in use. Software is being evaluated to allow CCCS to detect financial aid fraud.

Compliance with Program and Regulatory Requirements

As this risk is broad, several initiatives have taken place or are planned to ensure the System remains compliant with program and regulatory requirements:

- Centralization of Title IX investigations to ensure compliance with regulations and consistency in the Title IX process and updates to System Procedure 19-60a, Civil Rights and Sexual Misconduct Resolution Process, were made to comply with the new Title IX regulations.

- Progress continues to be made in digital accessibility. Several tools and trainings are now available to assist in compliance with digital accessibility laws and a new position, Digital Accessibility Specialist, was approved for FY 2025.

- Training on regulatory requirements continues including those applicable to accessibility of instructional materials, grant compliance requirements, and Title IX requirements.

- Various monitoring functions, including grant management audits, Civil Rights monitoring reviews, and Perkins monitoring reviews are performed to ensure compliance with program and regulatory requirements.

Information Security

The Information Technology department continues to make progress on several projects to ensure data is stored and transmitted safely:

- The Information Technology Security Project is on-going. 24/7 cybersecurity monitoring is occurring. The security plan and incident response plan have been drafted and are in various states of implementation and revision.

- In FY 2025, a project to automatically terminate system access for most types of employees will be completed.

- Most of the necessary Cybersecurity procedures have been completed and implemented and are failing into the normal rotation for revision. A cybersecurity audit occurred in Fiscal Year 2023. Findings from that audit that can be resolved have been resolved. In FY 2025, BP 6-10 and SP 6-10 will be updated to include the Cyber Incident and Information Security Plans. In addition, System Procedure 6-10G, Bring Your Own Device, will be completed and adopted.

- Ongoing training, including regular email reminders, for System Office and college staff is provided covering phishing, passwords, safeguarding, and protecting data in addition to other topics. A special executive level training was provided to system and college executives. Compliance with the training is presented to the presidents annually. Internal phishing tests are performed periodically for the system office and all colleges. Employees who fail the phishing test are provided with additional training.