SUNY Orange Policies

Policy Number	Policy Title
BP2.46	**Digital Data Protection and Cybersecurity Threat Preparedness**

Orange County Community College (SUNY Orange) is committed to securing and protecting the information within its possession. As an institution of higher education operating in New York State as a component of the State University of New York (SUNY), SUNY Orange must comply with federal and state confidentiality and information safeguarding laws, as well as meet data protection requirements imposed by its accrediting agency, the Middle States Commission on Higher Education (MSCHE).

SUNY Orange's core academic mission and strategic goals require policies, procedures, controls, monitoring and verifications to protect the information it possesses or transmits through the normal course of operations. In a digital environment, the broad range of information in SUNY Orange's possession that is central to the facilitation of academic programs, student services, and overall business operations has made such information one of the College's most important assets, requiring increased vigilance with respect to storing, sharing, and using data that builds on existing SUNY Orange policy and practice.

As a component of SUNY, SUNY Orange must meet the requirements of the SUNY Information Security Policy (SUNY ISP). The SUNY ISP mandates that SUNY institutions must:

- Adhere to SUNY policies, procedures, and state law regarding information assets and systems;
- Designate a Chief Information Security Officer (CISO);
- Develop an incident response process to ensure timely notification of campus leadership, including the campus President, of cyber security incidents and security breaches involving exposure of regulated or personally identifiable data;
- Ensure timely notification of SUNY Administration officials in the event of a critical suspected or actual information breach or cybersecurity incident;
- Complete the annual Self-Assessment Questionnaire disseminated by SUNY's CISO;
- Provide annual cybersecurity training to all individuals who access SUNY Orange information assets and systems;
- Ensure encryption of SUNY Orange information and information systems, as appropriate;
- Adopt campus specific policies regarding information security as appropriate;
- Require that any third parties who will store data, both paper and electronic, on behalf of SUNY Orange, have insurance in place to cover losses in the event of an information security or breach incident consistent with New York State law;
- Continually assess and monitor vulnerability of information security. (SUNY encourages all campuses to participate in the SUNY Security Operations Center to help with this assessment and monitoring); and
- Obtain breach insurance for the costs that result from an information security breach consistent with SUNY guidelines. Generally, breach insurance will cover costs that flow from breach discovery, mitigation, notification, and liability costs.

As an institution of higher education receiving Title IV funding from the federal government, SUNY Orange must meet the requirements of the Graham, Leach, Bliley Act Safeguard Rules: The GLBA mandates that the College:

- Designate a GLBA program coordinator or CISO;
- Identify and assess potential risks associated with the protection of covered data (including an annual risk assessment the results of which are formally communicated to the institution's governing board);

- Design and implement a Safeguarding Program to control risks identified in annual risk assessments. The safeguarding program must include the following elements:
    - Employee Management and Training;
    - Information Systems Security;
    - Safeguarding paper and electronic records containing covered data;
    - Oversight of Third-Party Service Providers;
    - Detection and Testing procedures; and
    - Regular Program Review and Revision.

The Board of Trustees directs the President to develop such procedures as to fairly implement this policy. The Board also directs the President to provide updates to the Board regarding results of the annual risk assessment as soon as is practical upon completion of the assessment.

Approved: Feb. 21, 2024