Ohio Administrative Code

Rule 3358:5-11-19 Information technology security policy.

Effective: October 23, 2015

In order to fulfill its mission of instruction and providing value to the community, the college is committed to providing a secure yet open network that protects the integrity and confidentiality of information while maintaining its accessibility.

(A) Information technology (IT) assets are comprised of computing equipment, network infrastructure, operating systems, applications, data, and all technologies that support the information and computing needs of the college.

(B) The college is responsible for the security and integrity of data it acquires about employees, independent contract workers, students, board members, student and employment applicants, and users of its facilities.

(C) IT assets must be protected from various security threats such as theft, vandalism, virus infections, denial of service attacks, and other activities that would breach their confidentiality, compromise their integrity, or prevent their availability.

(D) Appropriate controls must be used to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope with complexity from extensive security installations to protect a room or facility where server are located to simple measures taken to protect a user's display screen.

(E) Appropriate security measures for authentication, authorization, and accounting shall be implemented and maintained to ensure the confidentiality, integrity, and availability of IT assets and the security of information.

(F) While the implementation of security measures is needed to protect the colleges IT assets, too much security could limit usability and cause intolerable inconvenience to the users. The security measures must balance between restrictions and convenience as well as the cost to implement

security measures.

(G) The college shall implement measures to make the college compliant with federal, state, and payment card industry (PCI) local requirements for IT security.

(H) The college shall designate an information security officer (ISO) who is responsible for compliancy to protect the IT assets of the college and the security of personal information.

(I) Departments shall work with the ISO to ensure that the IT assets in their possession are secured as specified in the IT security procedures.

(J) All college employees, independent contract workers, students, and board members shall be appropriately informed of the colleges IT security policy and procedures.

(K) Failure to comply: Violation of any of the Clark state IT security policy and procedures may result in disciplinary or other appropriate action.

(L) User accounts and access to network assets can be revoked at any time.