Ohio Administrative Code

Rule 3342-9-03.1 Administrative policy regarding electronic information security.

Effective: December 1, 2020

(A) Purpose. The purpose of this policy is to enable the use of innovative technology by members of the university community while utilizing available resources to mitigate the risk of unauthorized access or disclosure. All computer systems either accessing or storing institutional data or operating on the university network must meet the information security standards as defined or otherwise referenced in this rule.

(B) Definitions.

(1) Application. A set of one or more computer programs designed to permit users to perform a group of coordinated functions, tasks, or activities. Examples of applications include but are not limited to: student support systems, administrative support systems, databases, and other application programs installed by the user or administrator on a device or server. For the purpose of this rule, covered applications are limited to those applications running or installed on university-owned information technology, on any server and/or storage device used to hold or transmit institutional data, or any cloud-based server and/or storage device.

(2) Physical server. A dedicated physical computer on a network that is capable of accepting requests from multiple university clients and providing responses accordingly.

(3) Virtual server. A server created through the use of software known as a hypervisor that allows a single physical computer to be partitioned into multiple server computing units.

(4) Storage device. A device used for recording and storing information (i.e. institutional data).

(5) Network attached storage device. A computer connected to a network that provides only file-based data storage services to other devices on the network.

(6) Firewall. A part of a computer system or network that is designed to block unauthorized access

while permitting outward communication.

(7) Institutional data. All data created, collected, maintained, recorded or managed by the university, its staff, and agents working on its behalf. It includes data used for planning, managing, operating, controlling, auditing and reporting on university functions. When appropriate, institutional data may also include research data that contains personally identifiable subject information, or proprietary university information.

(C) Scope. This policy applies to all student employees, faculty, staff, (collectively university stakeholders) and third parties acting on behalf of Kent state university as well as any other university affiliate authorized to access or is in possession of Kent state university institutional data and IT resources. This policy applies but is not limited to all computer systems (applications, physical servers, virtual servers, and storage devices) that process or store university information. The policy applies both to computer systems that are run locally at Kent state university campuses and those that are hosted or maintained by outside vendors. Exceptions to this policy must be approved by the vice president for information technology and formally documented. Exceptions will be reviewed on a periodic basis and may be withdrawn at the discretion of the vice president for information technology.

(D) Procedures.

(1) The division of information technology (IT or information technology) is responsible for documenting the required security standards, updating on a periodic basis, and posting to the IS website at security.kent.edu. (a) Such security standards as adopted and maintained by the division of information technology are intended to ensure adherence to the standards set forth by existing laws and regulations, such as but not limited to: sections 1349.19 and 149.43 of the Revised Code; the Family Educational Rights and Privacy Act; and the Health Insurance Portability and Accountability Act.

(2) Existing computer systems (applications, servers, and storage devices) will be audited against the current standards.

(3) All new requests for computer systems (applications, servers, and storage devices) must be

reviewed by information technology to ensure the proposed system meets the security standards.

(4) University stakeholders must receive prior approval from the division of information technology before utilizing externally managed services, applications, and servers.

(a) Vendors of externally managed services and applications shall be required to complete the vendor security checklist prior to engagement of such resources or transmission of institutional data. Such checklists must be reviewed by IS.

(b) Service agreements and terms of use shall be submitted by the requesting university stakeholder for review by information technology and other university stakeholders as required under rule 3342-5-04.1 of the Administrative Code.

(c) Any storage of institutional data with external service providers requires the prior approval of information technology.

(5) Servers and network-attached storage devices operating on the Kent state university network shall be secured according to the risk they pose to institutional data, to critical university processes, or to the ongoing compliance of the university to state, federal or other regulations.

(a) Servers and network-attached storage devices will be located in the data center if they:

(i) Contain sensitive personal identifiable information (PII);

(ii) Fall under state, federal, or other regulatory compliance obligations;

(iii) Directly integrate with other servers located in the data center;

(iv) Provide mission-critical functions to departmental faculty, staff, or to students; or

(v) Provide or impact financial-related processes.

(b) Access to the data center shall be controlled by IS operations staff.

(c) All data center devices shall reside behind IS-managed firewalls.

(d) Remote access shall be approved and managed by IS office of security and access management.

(6) All applications are subject to vulnerability assessments by IT. In the event of the identification of a critical vulnerability, IT shall require remediation in order for the user and/or server/storage device to remain on the network.

(7) The use or storage of sensitive institutional data (including but not limited to personally identifiable information, or other information protected from unauthorized disclosure by law, regulations or policy) on any server or storage device for any purpose must adhere to the processes, standards, and requirements as directed by IT office of security and access management.

(8) Domain names other than kent.edu acquired by university stakeholders for the operation of applications must be obtained and registered through information technology.

(9) Violations of this policy may result in suspension or loss of the users access to computing, storage, or network resources, with respect to institutional data and university-owned information technology.