Ohio Administrative Code

Rule 3342-9-02.1 Administrative policy regarding responsible use of information techology.

Effective: December 1, 2020

(A) Purpose. To ensure compliance with the university policy on responsible use of information technology, Kent state university establishes the following administrative policy which supplements university policy and any guidelines or regulations developed by individual units of the university, as well as applicable federal and state laws.

(B) User responsibilities.

(1) University assigned accounts ("UserID"), computer and network access accounts are for the personal use of that individual only. Accounts are to be used for the university-related activities for which they are assigned.

(2) Sharing of access. Computer accounts, passwords, and other types of authorization are assigned to individual users and should not be shared with others. Individual users are responsible for the use of their accounts. If an account is shared or the password divulged, the holder of the account may lose all account privileges and be held personally responsible for any actions that arise from the misuse of the account.

(3) Unauthorized access. Individual users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.

(4) Termination of access. When individual users cease being a member of the campus community (i.e., withdraw, graduate, or terminate employment or otherwise leave the university), or if an individual user is assigned a new position and/or responsibilities within Kent state university, access authorization may be reviewed. Users must not use facilities, accounts, access codes, privileges or information for which they are not authorized.

(5) Circumventing security. Users are prohibited from attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to

intercept or decode passwords or similar access control information.

(6) Breaching security. Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Kent state university computer or network is prohibited. Breach of security includes, but is not limited to, the following:

(a) Creating or knowingly propagating viruses;

(b) Hacking;

(c) Password cracking;

(d) Unauthorized viewing of others' files;

(e) Willful modification of hardware and software installations.

(7) Abuse of campus computer resources is prohibited and includes, but is not limited to:

(a) Unauthorized monitoring. A user may not use computer resources for unauthorized monitoring of electronic communications.

(b) Spamming. Posting a personal or private commercial message to multiple list servers, distribution lists or news groups with the intention of reaching as many users as possible is prohibited.

(c) Private commercial purposes. The computing and networking resources of campus shall not be used for personal or private commercial purposes or for financial gain

(C) Enforcement. Users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Violations will normally be handled through the university disciplinary procedures applicable to the relevant user. The university may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of university or other computing resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

(D) Reporting. Anyone who learns of misuse of software, hardware, or networks may report the activity by contacting the helpdesk at 330-672-HELP (4357) or helpdesk@kent.edu. The call will be referred to the appropriate unit.