3359-11-10.3 Information technology security and system integrity policy.

(A) Need for security and integrity.

The university abides by and honors its long history of supporting the diverse academic values and perspectives engendered in its academic culture, and the university deeply respects the freedom of expression and thought of its users. Although

(2) Providing for and implementing, in cooperation with the information technology security policy committee, a written system to investigate any violations or potential violations of this policy or any policy regarding system security and integrity, individually or in cooperation with any appropriate university, law enforcement, or investigative official;

(3) Enforcing the provisions of this rule;

(4) Keeping a record of system integrity problems and incidences;

(5) Taking such emergency action as is reasonably necessary to provide system control where security is deemed to have been lost or jeopardized;

(6) Performing periodic security surveys;

(7) Performing checks of network systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment;

(8) Disposing of software or equipment, through appropriate methods, that university officials deem to be legal or proper where such equipment is not attached to or accessing university network systems;

(9) Ensuring processes are in place to remove all data before equipment is disposed or redeployed;

(10) Training personnel who work with university network systems;

(11) Keeping copies of all records and reports necessary to implement this rule;

(12) Coordinating and consulting with the office of general counsel, the office of the VPCIO and the information technology security policy committee;

(13) Implementing decisions of the university concerning security; and

(14) Providing reports directly to the CIO and the respective vice president in any area where any security violation or potential challenge to security occurs.

(C) Information technology security policy committee.

(1) The CIO shall appoint an information technology security policy committee ("ITSPC") consisting of at least one member from each of the divisions represented by a vice president at the university.

3359-

communications equipment by department staff and students is prohibited, without the prior approval of the director of network and communication services.

Effective:	06/27/2016
Certification:	_____ Ted A. Mallo Secretary Board of Trustees
Promulgated Under:	111.15
Statutory Authority:	3359.01
Rule Amplifies:	3359.01
Prior Effective Dates:	06/09/03, 06/25/07, 01/31/15