UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Digital Copyright Policy	**Coverage:** OUHSC
Policy #: Information Security-P#15.1.2	**Version:** 2.1
Regulation: DMCA, State of Oklahoma	**Approved:** 05/06/07
Effective: 05/09/07	**Revised/Reviewed:** 11/14/2014

Policy Summary:	Copying, storing, and/or providing transport of digital material in a manner that violates the copyright associated with the digital material on or with any University information system resources is strictly prohibited.
Purpose:	This policy reflects the University's commitment to identify and implement security controls that will keep the risks to information system resources at reasonable and appropriate levels.
Policy:	Persons and/or devices found to be violating the copyright of any digital material shall have their network access restricted according to the *Information Systems Access Removal Procedure* until Information Technology has obtained evidence of compliance.
	The removal of the copyrighted material, along with file-sharing/peer-to-peer (P2P), reverse engineering, serial generators, software cracks or any other software enabling the violation of digital copyrights must be verified for all computing devices (University or privately owned) that connect to a University network. Failure to provide this evidence will result in the loss of network access per the *Information Systems Access Removal Procedure*.
Scope/Applicability:	This policy is applicable to all OUHSC workforce members, as well as any computing device connecting to the University network.
Regulatory Reference:	Digital Millennium Copyright Act of 1998, The Higher Education Opportunity Act (Public Law 110-315) (HEOA),State of Oklahoma Information Security, Policy Procedures Guidelines
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	Each department that maintains information systems and electronic media is responsible for complying with this policy.
Related Policies:	Information Systems Network Access Removal Procedures
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.
Procedures:	Each department that maintains information systems and electronic media is responsible for developing processes and procedures for complying with this policy.