

APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES

POLICY SUMMARY

within the parameters defined by this policy and its accompanying standards of appropriate use. These IT Resources, which include computers, servers, networks, electronic mail and telephonic services, data and data such use must comply with all applicable federal and state laws and regulations, Arizona Board of Regents and

REASON FOR THIS POLICY

Clear standards for the appropriate use of IT Resources promote institutional efficiency and effectiveness, enhance individual accountability for ethical and lawful use and help mitigate risk.

ENTITIES AFFECTED BY THIS POLICY

All units of the University community

WHO SHOULD KNOW THIS POLICY

All users of University IT Resources including faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, collaborators, volunteers, or members of the general public

DEFINITIONS

Account: a defined username with an associated Authentication Method that provides access to an IT Resource as the specified username.

Authentication Methods: the technical process used to determine the validity or legitimacy of a Digital Identity, updated periodically to reflect best practices in security management. Security methods are approved by the

Authorized Use: utilization of the IT Resources by an Authorized User in a manner consistent with, or in furtherance of, the mandates, standards, -related contracting and licensing agreements.

Authorized User: a person who has truthfully identified themselves and their purposes and to whom the University person accessing the public information services through a network connection open to the general

Digital Identity: a set of attributes stored as electronic data that represent or describe a person, device, or service. These attributes may include, but are not limited to, a name, an electronic mail address, login credentials, or similar identifying information that when, taken together, unmistakably describe and identify the person, device, or service.

_____ : any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University, regardless of ownership, location, or access method. These resources are referred to herein as

Sensitive Information: all information that should remain private or confidential as designated by the University or as required by law, including, but not limited to, educational and student conduct records, social security numbers, credit card or banking information, regulated research data, and health care provider records. Sensitive Information includes, but,

