Responsible Executive: Chief Information Officer
Responsible Office: Information Technology Services
Effective Date: April 7, 2021
Last Revised: August 19, 2022

ACCESS MANAGEMENT

POLICY SUMMARY

Management (IAM) Program. It guides actions related to University Information and the information

Community Members share the collective responsibility to protect access to University Information and IT Resources from harm through careful adherence to these requirements, which are designed to support the information-sharing needs of an academic culture.

REASON FOR THIS POLICY

University Information is a valuasign0.00000912 0 612 792 rewBT/F 9.96 Tf1 0 0 1 57.6 497.11 Tm737 rg rg99.792 rewBity to

RESPONSIBILITIES

Chief Information Officer: in collaboration with the Director of Information Security Services, update as *Access Management Standards*.

Data Stewards: perform periodic reviews of access levels, group memberships, sponsored affiliates, and role assignments to ensure eligibility.

Director, Information Security Services: reporting to the CIO, is responsible for working with the roles identified herein to develop and implement security policies, procedures, protocols, and standards in support of this policy and the Information Security Program; is responsible for working with individuals, departments, and administrators to implement and enforce this policy and serves as chair of the Information Security Committee.

Identity and Access Management Team: review and enforce access policies, standards, business rules and systems that manage and grant access to IT Resources; perform periodic reviews of access control systems to ensure existing granted accesses are still appropriate.

System Administrators and Technicians: ensure the effective implementation of this policy; maintain the privacy and confidentiality of sensitive information seen or obtained in the normal course of their work; report suspected or actual violations of the University IT policies to the appropriate University authority; perform periodic reviews of access levels, group memberships, sponsored affiliates, and role assignments to ensure eligibility.

University Community Members: familiarize themselves to and implement, within their respective areas of responsibility of jurisdiction, these policies and standards to protect University IT Resources.

PROCEDURES

Affiliate Account Request

Electronic Peoplesoft Administrative Security System (EPASS)

RELATED I

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

APPENDIX

None.