Access to University Technology
Resources & Services Policy

Last Updated

June 2016
PURPOSE
Arizona State University (ASU) provides centrally managed information technology services and resources to employees, students, and other affiliates for activities related to its mission of teaching and learning, research, and service. The University only allows access to individuals and entities that are actively supporting the institution’s mission and goals.

This policy is a component of a larger overall strategy for Identity Management (IDM), a program identifying individuals affiliated with the University in various ways and controlling their access to University resources and services by associating individual rights and restrictions with their established identity.

Two components integral to managing access to ASU’s information technology resources and services include authentication and authorization. Authentication is the means of verifying the identity of an individual. Authorization determines what an authenticated user is allowed to do or have access to. This policy applies to authentication and authorization of ASU managed resources.

Individuals or departments of the University who are in a position to access or authorize access to University-owned information technology resources and services should familiarize themselves with this Policy.

SOURCE
• University Technology Office
• University Office of General Counsel

APPLICABILITY
• Students
• Faculty
• Staff
• Other Affiliates (Courtesy Affiliates)

POLICY
ASU grants access to University-owned information technology services and resources predominately through ASURITE UserIDs to members of the ASU community and persons affiliated with the University.

The University will determine the level of authorized access based on role, status or other criteria. The scope of access varies with affiliation and may change. The Chief Information Officer acts as the Owner for all basic technology services managed and supported by the University Technology Office (UTO) and may designate trustees as necessary. Access to other centrally orchestrated services are granted or revoked at the discretion of the applicable Date Trustee.

UTO is responsible for periodic access reviews. Responsible University officials must evaluate their sponsored affiliates annually to ensure they remain eligible for services.

VIOLATIONS AND ENFORCEMENT
The University reserves the right to suspend or block access to an account when the University deems necessary.

REFERENCE
• ASU Access to University Technology Resources Standard