

## Purpose

In order to fulfill the mission of providing technology support to students, faculty and staff, Arizona State University (ASU) must grant privileges to access the university's electronic information systems to appropriate information technology (IT) employees. This access imposes upon the employee the responsibility and obligation to use systems in an ethical, professional and legal manner that is strictly within his or her authorized job functions.

ASU is committed to advancing the ethical and responsible use of all information technology resources. The objectives of the ASU University Technology Employee Code of Ethics are to create a culture that fosters trust and a commitment to responsibility, excellence and institutional and personal integrity.

## Applicability

This standard applies to all information technology employees using ASU's computing, internet and communications resources, including faculty, staff (including student employees), contractors, vendors, consultants, temporary and other workers for ASU and its Component Units (Users).

This agreement applies to **all** electronic equipment such as desktop computers, laptops, tablets, smartphones, and phones as well as **all** systems owned, operated, or subsidized by the university, which may include, but is not limited to: student information systems; financial information systems; research administration systems; human resource systems; e-mail systems; file servers; online course management systems; and the local, wide-area and wireless networks.

## Standard

In exchange for the privileges granted, and as a condition of employment, information technology employees agree to abide by all [ASU IT policies](#) and [Academic Affairs Manual](#) including but not limited to [ACD125: Computer, Internet and Electronic Communications Information Management Policy](#) and [SPP801: Employee Conduct and Work Rules](#) with the understanding that the ASU administration may change, rescind or add policies with or without prior notice. Information technology employees will:

Protect the college, the university, and the infrastructure by:

- Promoting and preserving public trust and confidence in the information and systems.
- Promoting the understanding and acceptance of prudent information security measures.
- Diligently working to protect all internal, sensitive and highly sensitive data from unauthorized disclosure.
- Preserving and strengthening the integrity of the public infrastructure.
- Discouraging unsafe practices.

Act honorably, honestly, justly, responsibly, and legally by:

- Truthfully informing stakeholders as needed to ensure visibility into issues of concern.
- Observing all contracts and agreements, express or implied.
- Treating all constituents fairly, objectively, resolving conflicts of interest, considering public safety and duties to principals, individuals, and the profession in that order.
- Giving prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort.

Provide diligent and competent IT service to customers by:

- Preserving the value of their systems, applications, and information.
- Respecting their trust and the privileges that they grant you.
- Avoiding conflicts of interest or the appearance thereof.
- Seeking support and training to ensure competency and qualifications to perform duties where authorization is required

Advance the IT profession by:

- Taking care not to injure the reputation of other professionals through malice or indifference.
- Maintaining competence; keeping your skills and knowledge current.
- Giving generously of your time and knowledge in training others.

## Violations and Enforcement

Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU's computing, Internet and communication resources until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

## Standard Revision

This standard is subject to review and revision at the direction of, and only after approval by, Chief Information Security Officer. To offer suggestions and/or recommendations, contact the ASU Information Security Office at [infosec@asu.edu](mailto:infosec@asu.edu).