UTEP Standard 14: Information Services (IS) Privacy

14.1 Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University, or retirees have no expectation of privacy regarding any University Data they create, send, receive, or store on University-owned computers, Servers, or other Information Resources (IR) owned by, or held on behalf of, the University unless expressly stated by Regent's Rules or as provided by applicable privacy laws. UTEP Information Security Office (ISO) employees may access and monitor Information Resources for any purpose consistent with the University's duties and/or mission without notice. They may also be accessed as needed for the purpose of system administration and maintenance; for resolution of technical issues; for compliance with the Texas Public Information Act; for compliance with Federal and State subpoenas, court orders, or other written authorizations; to conduct business of the University; and to perform audits.

14.2 Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device. Users must understand that they have no expectation of privacy in any personal information stored by the User on a System Information Resource, including University email accounts.

14.3 To manage systems and enforce security, UTEP may log, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code §202 (TAC§202). UTEP may also capture user activity such as telephone numbers dialed and web sites visited.

A wide variety of third parties have entrusted their information to UTEP for business purposes, and all employees and users at UTEP must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

Users must report any weaknesses in UTEP computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management or the Information Security Office.

Users must not attempt to access any data or programs contained on UTEP systems for which they do not have authorization.

UTEP web sites available to the general public must contain a Privacy Statement. Please refer to UTEP's Web Privacy Policy for more information.

14.4 Revision History

First Draft:	April 3, 2002
Revised:	September 19, 2002
Revised:	July 29, 2003
Revised:	July 26, 2011
Revised:	May 24, 2017
Approved:	June 16, 2017
	Gerard D. Cochrane Jr., Chief Information Security Officer
Revised:	June 17, 2019 (addition of retirees)
Approved:	June 18, 2019
	Gerard D. Cochrane Jr., Chief Information Security Officer