

TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology
AREA: Computer and Information Technology

NUMBER: 04.06.03

TITLE/ SUBJECT: Computer Use Policy

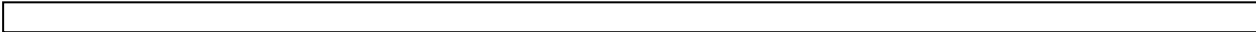
I.

PURPOSE AND SCOPE

III. DEFINITIONS

1. Computer

University is unable to unab l 292Ontee292On



- 1.5. When communicating with others via the university computer system, ensure that communications reflect high ethical standards, mutual respect and civility.
- 1.6. Obtain and adhere to relevant network acceptable use policies, including no transmittal of chain emails or spam.
- 1.7. Use communal resources wi



2.2. Supervisors shall promptly inform appropriate computer system administrators when employees have been terminated so that the terminated employee's access to University computer resources may be disabled

2.3. Supervisors shall promptly report ongoing or serious problems regarding computer use to the Office of Information Technology.

3. Misuse of computer Resources

7KH IROORZLQJ DFWLRQV FRQVWLWXWH PLVXVH RItlyWKH 80 prohibited for all Users:

3.1. &ULPLQDO DQG LOOHJDO DFWV 7H[DV 6RXWKHUQ 80 be used in support of or for illegal activities. Any such use will be reported and dealt with by the appropriate University authorities or law enforcement agencies. Criminal and illegal use may include, but is not limited to, unauthorized access, intentional corruption or misuse of computer resources, theft, obscenity, and pornography.

3.2. Failure to comply with laws, policies, procedures, licensing agreements, and contracts WKDW SHUWDLQ WR DQG OLPLW WKH XVH RI WKH 80

3.3. \$EXVH RI WKH 80QLYHUVLVW\TV FRPSXWHU UHVRXUFHV

3.3.1. Any act which endangers or damages specific computer software, hardware, program, network, security, or the system as a whole, whether located on campus or elsewhere on the global Internet;

3.3.2. Creating or purposefully allowing a computer malfunction or interruption of operation;

3.3.3. Injecting a computer virus on to the computer system;

3.3.4. Sending a message with the intent to disrupt the University operations or the operations of outside entities, for example chain email, spam and broadcast storm;

3.3.5. Printing materials that tie up computer resources for an unreasonable time period; and

3.3.6. Failing to adhere to time limitations which apply at particular computer facilities on campus.

3.4. Use of computer resources for personal financial gain or for a personal commercial purpose.

3.5. Failure to protect a password or account from unauthorized use.

--

3.6. Permitting someone to use another's computer account, or using someone else's computer account.

3.7.



5.1. As a State institution, the University must maintain its records in accordance with record retention schedules filed with the Texas State Library and approved by the State Archives Commission and State Auditor's Office. These schedules apply to electronic documents in the same way they apply to paper documents. Records should be kept only so long as is necessary. Employees must familiarize themselves with the retention periods that apply to the kinds of information they create or receive. Our retention schedules give us the right to dispose of University records so it is important that we follow them and destroy our records in a systematic way.

6. Review and Responsibilities

Responsible Party: Chief Information Officer

Review: Every 3 years, on or before September 1

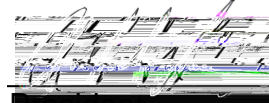
Forms

None

V. APPROVALS



Chief Information Officer



President

Effective Date 2/1/2018