

STOCKTON UNIVERSITY



PROCEDURE

Acceptable Usage Standards of Computing and Communication Technology

Procedure Administrator: Chief Information Officer

Authority: N.J.S.A. 18A: 64-8, N.J.S.A. 2C:20-23, et seq., 16 CFR Part 314, Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99)

Effective Date: December 29, 2018

Index Cross-References: Policy I-55 – Campus Conduct Code; VI-28 - Policy Prohibiting Discrimination in the Workplace

Procedure File Number: 4200

Approved By: Harvey Kesselman, President

Introduction

The Standards set forth below apply to all users of Stockton University computing and communication technology, which includes all email, computing, video, data and telecommunication hardware and software systems owned, leased, granted or used in name, conjunction or association with the University. The Standards also apply to the use of Stockton University computing and communication technology operated on a privately-owned computing device that is not managed or maintained by Stockton University. Use of Stockton University computing and communication technology must be limited to the users' status and function at the University.

Furthermore, users are advised not to consider any of their work, e-mail or electronic communication correspondence on University systems to be private. A violation of any of these Standards may result in revocation of usage privileges and/or appropriate disciplinary action under the University's Campus Conduct Code, and civil liability or criminal prosecution under applicable local, Federal and State laws and regulations (e.g., New Jersey Computer Crimes Act, N.J.S.A. 2C:20-23, et seq.).

The Standards of acceptable use of computer and communication technology follow below along with an explanatory discussion.

Standard 1 - Appropriate Use of Facilities

Authorized use of and access to the University's computing and communication technology is intended and permitted solely to support the legitimate educational, administrative and mission-centered programs of the University.

Discussion - Students may access University computing and communication technology to perform certain administrative functions needed for admission, advising, degree completion, financial aid, registration, residential life, tuition payment, as well as for course-related instructional and approved extra-curricular purposes. Residential students in good standing may access data and telecommunication facilities for personal use subject to this Procedure and related Residential Life policies and procedures. Members of the faculty and staff may access University computing and communication technology for institutionally-recognized or sponsored instructional, grant, or research purposes. Faculty and staff also may access academic and administrative computing technology, as needed, in accordance with their job responsibilities and professional development. However, personal use should be incidental and kept to a minimum. Limited access to computing and communication technology may be granted to users

Standard 4 - Reliability and Integrity of Facilities

Users of computing and communication technology shall not knowingly develop, use, or transmit through the University's technology system any programs, data, or technology that interferes with, infiltrates, or damages computing and communication technology, or violates any civil or criminal law.

Discussion – Users of the University's computer and communication technology shall exercise great care to prevent or protect the use of programs or utilities accessed through such technology and shall not engage in actions that interfere with, infiltrate, or damage such technology.

Users shall not engage in any activity that may lead to unauthorized access to systems, accounts, or data on the University's computing and communication technology. Additionally, users shall not attempt to circumvent or subvert system or network security measures. Further, implementing methods that mask network traffic for unauthorized or unlawful purposes is prohibited. Any defects discovered in system security must be reported immediately to the Chief Information Officer.

Standard 5 - Regulations

The University prohibits the use of computing and communication technology, including e-mail, phone, Internet, webpages, or systems with similar functions, to

re38.07 -1215 Td [-125(e)-5(nd f)o14(f)logn(obs)5(c)6(n c).(1(v)i)-3(ng,)7t,001 Tahar5(s)nt(o i)-3y,

Standard 6 - Proprietary Rights

Users shall respect and observe proprietary rights associated with software, data, and documents.

Discussion -

Users of e-mail should be aware that electronic mail is recognized as the equivalent of a formal memorandum. The University's e-

If the Chief Information Officer (CIO) or appropriate University supervisory authority believe that an alleged violation of these Standards or other regulations presents a risk to the integrity and/or the orderly conduct of the operation of the University's computing and communication technology, the user may be subject to restricted access or loss of access to such technology; disciplinary action under applicable University policies and procedures up to and including termination and/or expulsion from Stockton University; and where appropriate, civil and/or criminal liability.

Stockton University reserves the right to update or revise these Standards or implement additional policies and procedures in the future. Users are responsible for staying informed about and compliance with Stockton University policies and procedures