Office/Contact: Division of Technology and Security
Source: of

g. Reasonable administrative access to information technology and communications systems for purposes other than routine operation, troubleshooting, audit, maintenance, or security activities will be authorized by the Vice President for Technology & Security, successor, or designee, for good cause shown. The following circumstances illustrate, but do not limit, situations where access may be provided with or without notice in accordance with law:

    i. When requested by the University Office of General Counsel or SDBOR General Counsel, or an attorney designated by the University Office of General Counsel or SDBOR General Counsel for such purposes, in order to respond to a court order, subpoena, search warrant, or other such duly issued mandate;

    ii. When requested for necessary business purposes by an appropriate system or University officer, including, but not limited to, the University Office of General Counsel, SDBOR General Counsel, or an attorney designated by the University Office of General Counsel or SDBOR General Counsel to represent the University, the Assistant Vice President for Human Resources, or designee, or the Vice President with administrative responsibility and supervision over the administrative unit, functions, and staff that use the components of information technology systems for which access is sought;

    iii. When requested in furtherance of the legal, regulatory, or other applicable duties of the University or the system;

    iv. When requested in the course of investigating potential violations of policy, rule, or law; or

    v. When requested in the course of responding to a health or safety matter.

h. Use of the SDBOR or University's information technology systems is a privilege and requires that users act responsibly. Users must respect the rights of other users, respect the integrity of the systems, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements, copyright, patent, trademark, and trade secret laws. When accessing remote resources from the University, users are responsible for abiding by the following principles:

    i. Authorization to access the information technology systems is granted only to support the administrative, research, instructional, and service functions of the University; and

    ii. Authorized users may use the information technology systems for incidental purposes provided that such use does not directly or indirectly interfere with the University's operation of such systems, interfere with the user's employment or other obligations to the University, burden the University with noticeable incremental costs, or violate law or University or

action. Unacceptable use includes, but is not limited to, the following attempted or completed actions:

i. Infringing intellectual properties, including copyrights, patents, and trademarks;

ii. Disclosing trade secrets or other information resident in the systems that is private, confidential, or privileged;

iii. Violating intellectual property licensing agreements;

iv. Interfering with the normal operation of electronic communications resources, including, without limitation:

1. Modifying, damaging, or removing, without proper authorization, electronic information or communications system components or private electronic information or communications resources belonging to other users;

2. Encroaching upon others' access and use of the electronic information and communications system, as exemplified, without limitation, by sending excessive numbers of messages, printing excessive copies, running grossly inefficient programs when efficient alternatives are available, attempting to crash or tie up electronic communications resources;

3. Intercepting, monitoring, or otherwise conducting surveillance of communications, whether live or stored, of others;

4. Developing or using programs such as, but not limited to, viruses, backdoors, logic bombs, Trojan horses, bacteria, and worms that disrupt other users, access priv (e)11.2 (r)-13 Tc -3.6 (s)8uoiDe(ac0.9 (t)-p141 Td[o.d0.9 (s)-n&

1. Using email or other communication resources for broadcast or third party commercial advertising of meetings, events, and activities or to make announcements is prohibited. Email can be directed to specific individuals when this information comes from recognized University entities and organizations.

2. Broadcast advertising and announcement-making using email or other communication resources is permitted only in instances in which the University President or applicable Vice President considers the information to be critical to supporting the business activities of the University. Failure by individuals to distribute non-critical information in a timely matter via other communication means will not be relayed via broadcast email.

3. Advertising for events, meetings, or activities which are not officially sponsored by the University

m. Where the facts that would trigger disciplinary action under this policy may also constitute a criminal infraction under any state or federal law, it may be reported to responsible authorities, whether or not disciplinary action is initiated.

4. Responsible Administrator

   The Vice President for Technology & Security, successor, or designee, is responsible for the annual and ad hoc review of this policy. The University President is responsible for approval of modifications to this policy.

SOURCE: Approved by President on 11/17/2015. Revised, Approved by President on 01/30/2019. Revised; Approved by President on 02/22/2022. Revised 01/31/2024 (clerical).