COMPUTING SERVICES
Section: 135-5 Appendix A
Effective: 10/03/2022
Supersedes: New
Review Date: 10/03/2025
Issuance Date: 10/03/2022
Issuing Office: Executive Vice Chancellor Academic Affairs / Vice Chancellor – Chief Financial Officer

APPENDIX A – DISALLOWED ACTIVITIES
Last Updated 10/03/2022

Except as explicitly permitted by other University policies, the following are disallowed activities:

1. University IT resources may not be used for:

    a. unlawful activities;
    b. personal use inconsistent with Purpose/Allowable Use, above;
    c. uses that violate other University or campus policies or guidelines.

2. Users may not share authentication information, including usernames, passwords, login dongles, or passkeys. Individuals needing to grant access to email or calendaring accounts should leverage delegated access to provide assistants or schedulers with access.

3. Users of University IT Resources shall not, either directly or by implication, employ a false identity. However, this clause is not intended to preclude an authorized individual from conducting University business on behalf of another person (see 2., above). Where permitted by other University guidelines and policies, IT Resources may allow a User to use a pseudonym or to remain nameless when using that Resource. A pseudonym must not constitute a false identity.

4. Users may not circumvent approval or access request processes for granting access to systems or University data.

5. A User may not allow the User's family members or others to access IT Resources. This is prohibited regardless of where that IT Resource is physically located (e.g., a University laptop in a User's home). It is prohibited even when the use might be considered incidental personal use if done by the User.

6. Users shall not perform any intentional or unintentional action that denies another User access to IT Resources or consumes a disproportionate share of IT Resources. Users shall not take actions to circumvent quotas or monitors.

7. Users shall not copy or use any University-owned software, other intellectual property, or data unless they have the legal right to do so.

8. Users shall not send spam/unwanted bulk emails.

9. Users may not use any IT Resources to violate the security or privacy of others. Users may not engage in activities that aim to get around security or data protection mechanisms.

    Examples of prohibited activities include conducting phishing, pharming, or social engineering; distributing programs that are intended to disrupt, damage, weaken or spy on computer systems or network (including viruses or other malware); disruptively scanning, probing, sniffing, session

hijacking or traffic proxying; attempting to obtain passwords or login credentials for IT Resources that were not assigned to the User or for which they are not authorized.

Nothing in this prohibition is intended to interfere with research performed within the confines of a faculty-led research program with appropriate protections to the general campus network, data, and users.

10. Users shall not engage in “cyberstalking” or harassment using IT Resources.

11. It is prohibited to use University IT Resources for commercial purposes not under the auspices of the University or for personal gain, including running a business.

12. It is prohibited to use University IT Resources for political campaign activities.