Clayton State University Acceptable Use of Information Technology Assets and Services

Purpose

To enable delivery of reliable, efficient, and effective technology services, Clayton State University (CLSU) requires all users, including institutions, employees, students, contractors, guests, vendors and any other authorized person or organization ("users"), of all CLSU Information Technology (IT) resources and services to conduct themselves responsibly. IT resources and services include but are not limited to hardware, software, networks, data, the internet when accessed through CLSU resources, and communication systems, whether owned, leased, or otherwise provided by CLSU organizations ("resources"). Users of CLSU IT resources must respect the public trust that provides the resources; comply with federal, state and local laws; comply with CLSU policies, standards and directives; respect the rights and privacy of others; and respect the integrity of CLSU facilities and controls. This standard applies to all users of CLSU IT resources.

Requirements

Appropriate use of CLSU IT resources is an enterprise-wide undertaking necessitating that all users promote responsible behavior and create safeguards against abuse of CLSU IT resources. Therefore, all users are obliged to abide by the following general standards:

1) Use only resources for which authorization is granted. For example, it is a violation to:
    a. Prevent others from accessing a service to which they are authorized;
    b. Use resources for which the user is not specifically authorized;
    c. Use someone else's user account and password;
    d. Share user accounts and passwords with someone else;
    e. Use privileged access for purposes other than official duties; and
    f. Use unauthorized third-party software or information services to store, access or process CLSU information.
2) Use resources only for their intended purposes. For example, it is a violation to:
    a. Use resources for advertising or commercial purposes other than for official CLSU business;
    b. Misuse software to conceal anyone's identity or attempt to circumvent security safeguards;
    c. Interfere with resources that impair or inhibit the work of other users;
    d. Create or forward threats, hoaxes, chain letters or forged email, except to report them; and
    e. Intercept or monitor any network communications not intended for you without permission or in support of official duties.
3) Respect the privacy and personal rights of others. For example, it is a violation to:

a. Disclose information about faculty, staff and students in violation of federal, state, local law, directives or CLSU guidelines;
b. Access or attempt to access CLSU resources or other user accounts or credentials without authorization;
c. Monitor or tap data communications or traffic on CLSU IT resources without express permission;
d. Access or copy communications, data or files of other users without permission; and
e. Transmit, disseminate, sell, store or host material on CLSU resources that is unlawful, libelous, defamatory, obscene, pornographic, indecent, lewd, harassing, threatening, harmful, invasive of privacy rights, abusive, inflammatory, or otherwise objectionable.

4) Protect access, integrity, and confidentiality of CLSU resources. For example, it is a violation to:
    a. Release malicious software that damages or harms any CLSU resources, including systems or networks;
    b. Attempt to deliberately degrade performance or deny services of CLSU IT systems;
    c. Corrupt, misuse, alter or destroy information without authorization;
    d. Purposely seek or exploit security flaws to gain system or data access; and
    e. Store protected or confidential information in unintended or unprotected locations.
        i. Employees may store company-related information only in CLSU approved storage (CLSU Microsoft One Drive is the only approved storage location connected to the user domain account.)
        ii. Employees may not use cloud-based storage, apps or backup on state-owned equipment or endpoints that allows university-related data to be stored or transferred to unsecured parties or have not been approved by CLSU.
5) Respect intellectual property and copyrights of others. For example, it is a violation to:
    a. Use unsupported or expired software in violation of CSU guidelines;
    b. Download, use or distribute copyrighted materials without permission;
    c. Download, use or distribute pirated software, music, videos, or games; and
    d. Make or use more copies of licensed software than permitted.

Enforcement

1) Every user has an obligation to report suspected violations of this standard using the CLSU incident reporting procedures or to the HUB.
2) Furthermore, any user engaging in unethical and/or inappropriate practices that violate CLSU standards is subject to disciplinary proceedings that may include suspension of system privileges, expulsion, termination and/or legal action as appropriate.
3) If a user is suspected of violating CLSU standards or policy, any right to privacy may be superseded by CLSU's requirement to protect the integrity of IT resources, the rights of all users, and state assets.
4) The CLSU reserves the right to examine material stored on or is transmitted through IT resources to maintain appropriate standards of conduct and duty of care.

5) Clayton State University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities.
6) Depending on the individual and circumstances involved this could include the offices of Human Resources, Provost, Dean of Students, Legal Affairs, and/or appropriate law enforcement agencies.
7) Failure to comply with Clayton State University information technology policies may result in sanctions
    a. relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material);
    b. the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy);
    c. the individual's studies within the university (such as student discipline in accordance with applicable university policy);
    d. civil or criminal liability;
    e. or any combination of these.
8) If the determination of relation to the mission or determination of incidental personal use is unclear, the Chief Information Officer will coordinate with campus administration and the unit involved to help determine whether the activity in question is an appropriate use of resources.

References & Supporting Documents

- CLSU Security Policies
- CLSU Policies and Procedures
- USG IT Handbook & resources

Approvals

Print: William Gruszka Signed Bill Gruszka (Dec 17, 2021 08:31 EST) Date: 12/17/21

CIO

Print: T. Ramon Stuart Signed Ramon Stuart (Dec 17, 2021 14:30 EST) Date: 12/17/21

President