Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

This document defines the appropriate use of Clayton State University (CSU) computing resources by faculty, staff, students and guests.

Use of Clayton State Information Technology resources is granted based on acceptance of the following specific responsibilities:

Use only those computing and IT resources for which you have authorization.	**For example, it is a violation:** ▪ To use resources, you have not been specifically authorized to use ▪ To assist in, encourage, or conceal from authorities any authorized use and/or attempt at unauthorized use ▪ To use someone else's account and password or share your account and password with someone else ▪ To access files, data, or processes without authorization ▪ To purposely look for or exploit security flaws to gain system or data access
Protect the access and integrity of computing and IT resources.	**For example, it is a violation:** ▪ To use excessive bandwidth

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Use only those computing and IT resources for which you have authorization.	**For example, it is a violation:** ▪ To use resources, you have not been specifically authorized to use ▪ To assist in, encourage, or conceal from authorities any authorized use and/or attempt at unauthorized use ▪ To use someone else's account and password or share your account and password with someone else ▪ To access files, data, or processes without authorization ▪ To purposely look for or exploit security flaws to gain system or data access
	▪ To release a virus or a worm that damages or harms a system or network ▪ To prevent others from accessing an authorized service ▪ To send email that may cause problems and disrupt service for other users ▪ To attempt to deliberately degrade performance or deny service ▪ To corrupt or misuse information ▪ To alter or destroy information without authorization ▪ To cause intentional damage to computer systems

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Use only those computing and IT resources for which you have authorization.	**For example, it is a violation:** ▪ To use resources, you have not been specifically authorized to use ▪ To assist in, encourage, or conceal from authorities any authorized use and/or attempt at unauthorized use ▪ To use someone else's account and password or share your account and password with someone else ▪ To access files, data, or processes without authorization ▪ To purposely look for or exploit security flaws to gain system or data access
Abide by applicable laws and USG policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.	**For example, it is a violation**: ▪ To download, use or distribute copyrighted materials, including pirated software or music or videos or games ▪ To make more copies of licensed software than the license allows ▪ To operate and participate in pyramid schemes ▪ To upload, download, distribute, or possess pornography ▪ To upload, download, distribute, or possess child pornography

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Respect the privacy and personal rights of others.	**For example, it is a violation:** ▪ To use electronic resources for harassment or stalking other individuals ▪ To tap a phone line or run a network sniffer or vulnerability scanner without authorization ▪ To access or attempt to access other individual's password or data without explicit authorization
Respect the privacy and personal rights of others.	▪ To access or copy another user's electronic mail, data, programs, or other files without permission ▪ To disclose information about students in violation of CSU guidelines ▪ To acquire, modify, or distribute any information belonging to another individual without explicit permission

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Take appropriate precautions to preserve the integrity and security of resources	**Users agree to:** ▪ Safeguard their account and password ▪ Take full advantage of file security mechanisms ▪ Back up critical data on a regular basis ▪ Promptly report any misuse or violations of the Policy ▪ Use virus scanning software with current updates ▪ Use personal or hosted firewall protection ▪ Keep their operating system up-to-date ▪ Install security patches in a timely manner ▪ Assume full responsibility for any loss, damage, or destruction that us caused by negligence, misuse, abuse, or carelessness

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Users are therefore urged to take appropriate precautions such as:

- Safeguarding their account and password
- Taking full advantage of file security mechanisms
- Backing up critical data on a regular basis
- Promptly reporting any misuse or violations of the policy
- Using virus scanning software with current updates
- Using personal firewall protection
- Installing security patches in a timely manner

Violations

Every user of Clayton State University IT resources has an obligation to report suspected violations of the Appropriate Use Policy and its related policies, standards or guidelines. Reports should be directed to the HUB and/or the data owner responsible for the particular system involved.

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Users understand that any violation of this policy may call for corrective action as deemed necessary by the employee's supervisor, department head, or Vice President. Policy violation by students will be addressed by Student Judicial Affairs. Violators may be subject to local, state and/or federal prosecution.

A violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices, which may include, but are not limited to:

- Widespread infections from virus, worms, Trojan horse or other malicious code
- Unauthorized use of computer accounts and computer systems
- Unauthorized, intentional or inadvertent disclosure or modification of sensitive/critical data or infrastructure
- Intentional disruption of critical system functionality

- Intentional or inadvertent penetration of firewall
- Compromise of any server, including Web server defacement or database server
- Exploitation of other weaknesses, known or unknown
- Child pornography
- Attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or system or national security and
- Violations of state or USG security policies or standards that threaten or compromise the security objectives of the state or USG data, technology, or communications systems. See the USG IT_Handbook for more information.
- Any violation of the "Appropriate Use Policy"

Clayton State University
Appropriate Information Systems
Use Policy

Revised July 2017

Incident Response

Every user of Clayton State University IT resources has an obligation to report suspected violations of the Appropriate Use Policy for Computing and IT Resources, as well as any other Information Technology Services policies, standards or guidelines. Reports should be directed to itsecurity@clayton.edu and/or the data owner responsible for the particular system involved.