ACCEPTABLE USE OF COLLEGE COMPUTING RESOURCES

I. POLICY

Salt Lake Community College (SLCC) creates and maintains computing, networking, and information resources to conduct and support the instructional, research, and administrative activities of students, faculty, staff, and the college community. This policy ensures the proper use of resources in accordance with the mission of SLCC and protects the college community and college property. Every user of SLCC resources is required to know and follow this policy.

II. REFERENCES

A. Standardized Systems Prescribed by the Board, Utah Code Ann. 53B-6-102.

B. Computing Systems Program, Utah State Bd. of Regents r. 341.

C. Information Management, Utah State Bd. of Regents r. 343.

D. Information Technology Resource Security, Utah State Bd. of Regents r. 345.

E. Institutional Business Communications, Utah State Bd. of Regents r. 840.

III. DEFINITIONS

A. Authentication Credentials: user ID and PIN, username and password, or other secrets or keys used to gain access to a restricted resource.

B. Enterprise Email Service: The email system which SLCC uses to engages in official business, such as @slcc.edu. This definition does not include a separate, affiliated email service SLCC may offer to alumni or other groups.

C. Incidental Use: Authorized personal use of a restricted resource resulting in an insignificant private gain. This use does not include external business transactions of a personal nature.

D. Institutional Business Email Communications: Email communications sent by an employee or another authorized individual on behalf of SLCC as part of their duties, and other email communications the college has designated as business communications.

E. Political Purposes: Any act done with the intent to influence any person to vote or refrain from voting for or against a candidate, judge, ballot measure, ballot proposition, or to solicit campaign contributions.

F. Resource: Any electronic hardware or software that makes the storage or use of information possible.

G. Restricted Resource: Resources available only to individuals in particular roles within the college community.

H. Standards and Best Practices: Computer device maintenance that includes operating system and application patching, anti-virus and malware protection, firmware updates, peer-to-peer networks, etc.

I. User: Faculty, staff, students, and members of the college community who access college resources.

IV. PROCEDURES

A. General Use

1. The office of Information Technology is responsible for administering, maintaining and monitoring the college's computing resources.

2. SLCC computing, networking, and information resources are provided as a service for use by faculty, staff, students, and the college community in a responsible manner that is within the capacity of the resource and consistent with the mission of the college and public trust.

3. Individual departments have the discretion to establish reasonable and appropriate conditions of use of resources. Departmental conditions of use must be consistent with this policy, although they may provide additional detail, guidelines, or restrictions.

4. User-owned equipment connected to the college network must be properly registered and managed in compliance with standards and best practices to protect against technical vulnerabilities that could allow outsiders to gain access to resources.

B. Credentials

1. Authentication credentials are assigned as an access privilege for restricted resources that are relevant to the role of the user.

2. Users must maintain credentials that are compliant with college requirements and best practices as described here.

3. Credentials must be protected from use by anyone other than the assigned individuals. Users are prohibited from sharing credentials with anyone.

4. SLCC's Office of Information Technology may revoke credentials to protect resources.

C. User Responsibilities

1. Use of college resources must not disrupt, distract from, or interfere with college business.

2. Users are responsible for activity originating from their resources which the user can reasonably control.

3. Users must obey relevant federal, state, and local laws with special attention to copyright, defamation, harassment, obscenity, child pornography, privacy, and government property laws. SLCC will cooperate with law enforcement agencies when allegations of violations are made.

4. Users must treat college data and information maintained by other users as confidential unless otherwise classified under a federal or state law, statute, regulation, or college policy.

5. Users must protect the integrity of the resource and the confidentiality of stored and transmitted data by following directions specific to the resource being used and the data being accessed.

6. Users must report the theft or misuse of college computer and technology resources to the college's department of Public Safety and the college's Office of Information Technology.

D. Prohibited User Activities

Users must not:

1. access or attempt to access computer systems using college resources without authorization;

2. use college resources in a way that would violate any college policy;

3. damage or attempt to damage college resources;

4. deliberately or recklessly create or disseminate malicious programs which would harm the integrity of college resources;

5. release confidential, private, controlled, or proprietary information without authorization;

6. monitor or attempt to monitor the use of college resources without authorization;

7. use college resources in a manner that interferes with the ability of other users to access college resources;

8. knowingly falsely identifying themselves on college resources;

9. use unauthorized applications designed to obfuscate the nature of web traffic, unless the use is for a legitimate educational purpose;

10. engage in illegal activities while using college resources; or

11. engage in any other activity that damages the college's reputation.

E. Email

1. When conducting college business, users must use only the college's enterprise email system.

2. Users are prohibited from using any private or non-enterprise email service for institutional business email communications.

3. Users are prohibited from sending unauthorized, unsolicited email communications, including spam or other advertising material, to users who did not specifically request such communications.

4. Users are prohibited from using email for political purposes.

F. Social Media

1. Users who post to social media from the college's enterprise email system (@slcc.edu) must include a disclaimer stating the user's opinions or statements are strictly the user's own unless the user is authorized to represent the college on social media.

2. Users are personally responsible for user-generated content published to social media.

3. Users are prohibited from publishing information to social media that violates federal, state, or local laws, including the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), Utah's Government Records Access Management Act (GRAMA), and copyright and trademark protections.

G. Incidental Personal Use

1. Users must use college issued restricted resources for purposes consistent with their particular role within the college community.

2. Users may use a college issued restricted resource for incidental personal use provided that the use is lawful and that each of the following conditions are met:

   (a) There is no additional accrued cost to the college as a result of the use;

   (b) The use does not interrupt nor interfere with college operations; and

   (c) The use is not for substantial personal profit, gain or for the promotion of non-college sponsored commercial ventures.

H. Privacy

1. College resources are the sole property of the college, and all data and information may be accessed by the college at any time. By using college resources, users agree they have no right or expectation of privacy in those resources.

2. College resources owned and managed by SLCC are as secure as the college can make them. Users should take extra precaution to protect their own privacy, ensure confidentiality of their personal identifying information, and guard against the loss or destruction of their intellectual property.

3. The college reserves the right to monitor any aspects of its resources at any time without notice and user's permission.

4. Records identified on college resources may be subject to GRAMA.

I. Enforcement

1. SLCC may take any action reasonably related to the performance of college business or the protection of college resources, college property, or users, including disconnecting devices; revoking or prohibiting access to resources; or monitoring, examining, or disclosing data or information.

2. Corrective action or academic sanctions for violations of this policy will follow the college's Corrective Action Policy for college employees and Code of Student Rights and Responsibilities for students.

3. Users who are not faculty, staff, or students of the college may have their access to resources revoked for violations of this policy.

J. Warranties

1. SLCC makes no warranties of any kind concerning resources.

2. SLCC is not responsible for damages resulting from the use or misuse of college resources, including loss of data, hacking, or service interruptions.