I. Purpose

The purpose of this policy is to protect the College network and information resources. Inappropriate use exposes South Texas College to risks including virus attacks, compromise of network systems and services, and legal issues. The intent of this policy is not to impose restrictions that are contrary to the institutions established culture of openness, trust and integrity. South Texas College endeavors to protect employees, students and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of everyone at the college who deals with information resources.

II. Policy

Scope

This policy applies to all users of information resources, including but not limited to: students, employees, Board members, contractors, consultants, temporaries and guests, including all personnel affiliated with third parties, whether on campus or from remote locations.

Passwords for college information resources are considered as a type of key to access an information resource. For this reason, passwords are considered as an extension of an information resource that are a direct responsibility of the assigned individual.

Acceptable Use

State law provides protection against abuse of information resources or against unauthorized use. In the same manner, the College shall define activities that are not acceptable and that might break the law, impact operations or create a negative environment.

1. Responsibilities of User of College Information Resources
   a) Protect information that is classified as confidential or protected by law.
   b) Protect the user identification and password that is assigned or updated.
   c) Adhere to the Information Security Mobile Device Security Standard when connecting personal devices to college information resources.
   d) Immediately report lost or stolen devices that are owned by the College or personal devices that contain College data.
   e) Respect intellectual property rights.
   f) Adhere to the terms of software licensed by the College or installed on College information resources.
   g) Use information resources in a manner that complies with State and Federal law.

2. Prohibited Uses of College Information Resources
   a) Sharing the password for your College user accounts.
   b) Attempting to gain or gaining unauthorized access to information resources.
   c) Sending unsolicited email messages unrelated to College functions.
   d) Intercepting electronic communications.
   e) Disabling or tampering with the security controls applied to information resources.
   f) Performing actions on information resources that result in disruption or performance degradation.
   g) Transmitting or displaying media content in a manner that violates the College’s policy, including, but not limited to, Policy 4216 Harassment, Discrimination, and Sexual Misconduct.
h) Copyright infringement by illegally downloading, streaming, or sharing protected material.

i) Use of information resources for personal profit, commercial reasons, non-College fundraising, political campaigning or any illegal activity, with the exception of activities sponsored by the College.

j) Intentionally or knowingly installing, executing, or providing to another user, a program or file that could result in the damage or unauthorized modification of an information resource.

k) Personally owned devices can only connect via our wireless network.

Administrative Discretion
The Board of Trustees grants the President and the Administration of the College the authority to develop and adopt guidelines implementing this policy and assuring that Users are advised of the guidelines and the penalties for their violation.

Enforcement
Any User violating this policy or related guidelines is subject to immediate disciplinary action, which may include loss of privileges, termination of employment, student expulsion or termination of a contract. Notwithstanding the foregoing, a User violating this policy may be subject to civil damages and criminal liability.

Monitoring
To ensure compliance with College policies and laws related to the use and security of information resources, information security personnel have the authority and responsibility to monitor network traffic and use of information resources. Electronic mail transmissions and other use of the College’s information resources shall not be considered private and may be subject to Public Information Requests.

III. Definitions

Information Resources – Any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, handheld computers, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

User – A person or entity which has been given the privilege to access the College’s Information Resources.

IV. History

<table>
<thead>
<tr>
<th>Origination Date Approved by Board</th>
<th>March 27, 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Reviewed and Approved by Board</td>
<td>March 27, 2018</td>
</tr>
<tr>
<td></td>
<td>April 23, 2019</td>
</tr>
</tbody>
</table>