Procedure 9.0303

System Security Procedure

System security is the responsibility of all employees.

Administrative or network access is to be closed prior to users leaving their work areas, either by logging out or locking their workstations. All users will be expected to follow the security guidelines as described by the Institutional Information Processing System users group (IIPS) Information Security Standard.

All workstations shall be safeguarded from unauthorized access when left unattended. The College shall configure all workstations to require a password-protected screen saver after a maximum of thirty (30) minutes of inactivity.

The following personnel have been approved by the President for authorizing access and assigning rights for the indicated areas:

Financial	Records	VP of Administrative Services
Human Resources	Records	VP of Administrative Services
Registration and Student	Records	VP of Student Services
Electronic	mail	Network Administrator

Access to Financial and Human Resources Records as well as Registration and Student Records must be annually authorized by the respective data owners and the employee’s direct supervisor.

User passwords shall be changed at least every ninety (90) days. Passwords for administrative accounts, including any user accounts with more privileges than those of a typical user, shall be changed at least every thirty (30) days whenever possible but must not exceed every sixty (60) days.

Administrative user passwords must be changed at least once within a 13 week period. A user’s account will become inactive if users do not access their accounts during a 16 week period. All accounts that have been disabled for greater than 365 days shall be deleted.

Users are expressly forbidden to share passwords with anyone unauthorized for any reason. No user login or password is to be left in work areas.

A. General Polices

1. New equipment purchases for all College computers and peripheral technology require prior discussion and review of the system administrator and/or network administrator respectively and approval by the Director of Information Technology. Planning for departmental expansions and relocations should be completed on an annual basis.
2. Requests for LAN equipment are to be made to the network administrator.

3. Requests for stand-alone workstation computer repairs are to be made to the computer support coordinator.
4. New administrative software application development or program modifications are to be made to the system administrator in writing and a meeting scheduled to discuss implementation details.
5. Software for desktop computers will be reviewed by the related Vice President, network administrator, the customer support coordinator, and approved by the Director of Information Technology.
6. Problems with out-of-warranty hardware or software are to be brought to the attention of the system administrator or network administrator, respectively, prior to seeking help outside the College.
7. Software and Intellectual Rights: Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment and determination of form, manner, terms of publication, and distribution.

   Because electronic information is easily reproduced, respect for the work and personal expression of others is essential in computer environments. Violations of authors' integrity, including plagiarism, unauthorized access, and trade secret/copyright violations are grounds for sanctions against willful perpetrators.
   Unauthorized copying or use of software is a violation of federal law, a possible breach of a license agreement, and an act that may subject the offender to disciplinary action by the College setting and, additionally, both the employee and his/her employer to civil and criminal penalties.

   Faculty, staff, and administration will not copy software for use on an additional machine is prohibited unless expressed permission in writing from the publisher is received. The Information Technology department will manage software imaging, distribution and licensing issues.

   The College does not request, require, or condone the unauthorized copying or use of computer software. Therefore, such action should not be taken during employment with BCCC. Such actions may be subject to disciplinary action with the College and/or criminal prosecution.

8. Software Registration:

   All software purchased by the College remains the sole property of the College, Beaufort County, or the state of North Carolina. At no time does software purchased by school funds or developed on school equipment or time revert to individual ownership.

   Individually licensed copies installed on fixed media are considered in use on the one machine and are subject to re-licensing for use on subsequent computers. The terms of some State software contracts allow instructors and employees to load a companion product to home computers. These copies continue to be owned and controlled by the contract terms and cannot be shared outside of the campus community. Inquiries for such use should be directed to the network administrator.

Computer users shall not intentionally interfere with the normal operation of computer networks.

All additional requests for network access points where network ports are not currently available must be made to the network administrator.

References

Legal References: *Enter legal references here*

SACSCOC References: *Enter SACSCOC references here*

Cross References: Information Technology Policy

History

Senior Staff Review/Approval Dates: *11/6/13*

Board of Trustees Review/Approval Dates: *Enter date(s) here*

Implementation Dates: *Enter date(s) here*