Procedure 9.0301

Information Technology Procedure

A. General Use

Any member of the College Community with a valid Beaufort Community College ID Card (a "User") may use any of the computers in the student public access areas, except when these areas have been reserved. Users may also be supplied with a network mail account. Temporary access to Information Technology Resources may also be extended on a limited basis to campus visitors. The Community College reserves the right, in its sole and absolute discretion, to refuse access to its Information Technology Resources to any person who is not a member of the Community College Community.

All Users are responsible for helping to maintain a sound computing environment. Acts which serve to degrade Information Technology Resources, whether deliberate or otherwise, are prohibited. Beaufort Community College has the right to monitor, limit, or restrict specific technologies that disrupt or degrade Information Technology Resources.

Information Technology Resources are made available primarily for academic and administrative activities. Unauthorized use of Information Technology Resources for commercial purposes is prohibited.

Academic use of Information Technology Resources takes precedence over non-academic use.

Individuals should report any reasonable suspicion of computer security problems to the Director of Information Technology or any member of the IT staff.

Beaufort Community College reserves the right to limit or restrict any individual user's access. An Officer of the College or the Director of Information Technology may, without notice, authorize immediate removal of any user, data, file or system resource that may undermine the authorized use or security of the Information Technology Resources.

B. Physical Security

Servers, networking equipment, processing equipment and telephone equipment shall be located in secure locations requiring key card access. Only Information Technology department personnel shall have access to these secure locations and all access shall be recorded.

C. Virtual Security

A secure firewall shall control all external access to the core network. Remote user access to the core network shall be controlled via Virtual Private Network access that will be

granted and controlled by the Information Technology department upon Vice Presidential request and approval.

World Wide Web filtering shall be performed by a security appliance and will be in use on both the Core wired network and both the secured and open wireless networks.

Virus and malware protection shall be managed via an enterprise level solution. The definitions will be updated as available and deployed to the end user community via centralized delivery.

Authentication for network access shall be controlled by an enterprise level user identity system implementation.

References

Legal References: *Enter legal references here*

SACSCOC References: *Enter SACSCOC references here*

Cross References:

History

Senior Staff Review/Approval Dates: *Enter date(s) here*

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

Implementation Dates: *Enter date(s) here*