Charleston Research Institute
Policy Memorandum

Title: Computer Security Policy
Reviewed by: Board of Directors
Implementation Date: 11/14/2016
Next Scheduled Review Date: 11/14/2019
Approval: Amanda C. LaRue, Ph.D., Chairperson

Policy Statement:
Off-site managed servers are utilized, backed-up daily, and monitored periodically with access to the accounting system limited to the administrative employees required to use it.

Background:
CRI electronic data files are located on a remote server through Atlantic Computer Company systems using Sonicwall NSA firewalls which are fully compliant with FIPS 140-2.

Guidelines:
CRI uses passwords to restrict access to accounting software and data. Only duly authorized accounting personnel with data input responsibilities have passwords that allow access to the system. They are also are expected to keep their passwords secret.

User access to QuickBooks is restricted to the Executive Director and bookkeeper. Access to back-up files shall be limited to individuals authorized by management. Backups are regularly made on a daily basis.