Bon Secours Health System, Inc.
Richmond Region
Bon Secours Memorial College of Nursing

Title: Systems & Data Security	Policy No.: ADM 1.03	Date: 7/28/10 Rev.: 11/28/11, 8/1/15
Areas Affected: All BSMCON Personnel		Page 1 of 1

This policy is intended to support the protection, control, and management of information assets of the Bon Secours Memorial College of Nursing and covers data and information that is stored and shared in any way on databases, personal computers, and removable media (such as tapes, USB drives, etc.)

The College specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or causing loss of the College's information assets. It also prohibits using information assets to violate any law, commit any intentional breach of confidentiality or privacy, compromise the performance of systems, damage software, physical devices or networks, or otherwise sabotage the College's information assets. Downloading patient information to removable media (such as a USB drive) from the electronic health record is prohibited and subject to disciplinary action. Authorized users are responsible for minimizing risks and securing information assets within their control.

The College's designated system administrators will determine the scope of system access and usage based on each employee's current responsibilities and will expand, limit, or terminate system access based on changes in responsibility. All personnel are required to receive orientation and/or training from the designated system administrators prior to using any of the College's systems and to protect their login assigned ID#s and passwords.

The College's systems are backed up nightly and prior to any major system upgrades by either by a host company or Bon Secours' Information Services Division. The College also participates in Bon Secours' disaster recovery initiative and has redundant servers for its onsite systems. The Bon Secours Information Systems Division would implement their standard protocol for recovery operations should the need arise. Personnel are responsible for regularly backing up their non-systems data to a shared network drive in order to be included in Bon Secours' nightly back-up.

Protection of data is required by law and prevents potential liability, severe negative publicity, and long-term loss of critical College data. Personnel must secure data by having actual possession of an item (e.g., laptop, USB drive) at all times or locked in a secure place. If the device is a laptop or any portable storage media, it should never be left unattended in a classroom or conference room. Personnel should also lock their unoccupied offices and, when leaving the office for the day, should secure laptops and any other sensitive material in locked drawers or cabinets.

Reference Policy #_____

Approved by:

Signature	Dean, Finance & Administration Title	8/1/15 Date
Signature	Provost/VP Title	8.1.15 Date

Approval History:
Committees and Dates:
AD Administration – 7/10, 10/31/11
Policy Committee –7/28/10, 11/28/11, 8/1/15

Key words: _Systems Data Security