RADFORD UNIVERSITY

Clinical Simulation Center

Media Storage and Protection Policy

Original Date: April 2014 Reviewed: Annually
Last reviewed: May 2023

I. Purpose

Radford University is committed to maintaining a reliable and secure technology infrastructure. Secure storage of media where sensitive data is stored is critical to the security of University information. This policy provides guidelines for handling of sensitive data and protecting media from compromise.

II. Policy

Video storage records/media is physically secured in server room and logically secured using SimIQ simulation management software. The SimIQ System uses built-in password protection and access control protocols. SimIQ system password requirements comply with best practices recommended by "Code of Practice for Information Security Management". Access control provides multi-layered access for variety of roles from participant student up to Administrator level. Within each role access to data is limited by scope and/or by the time period during which access may be granted. Video files are purged from system within 2 years of student graduation.

III. Procedure:

1. Media owners are responsible for classifying their video sensitivity and for notifying system owners of the sensitivity and media protection requirements of the video they own.
2. Media custodians are individuals or entities that are in physical or logical possession of video for owners. Custodians are responsible for protecting the video in their possession from unauthorized access, alteration, destruction, or usage.
3. Video storage media containing highly sensitive data must be physically and logically secured.
4. Employees, who have approval to store any video on mobile devices, must receive security awareness and training specific to video media protection requirements.
5. Only authorized personnel are permitted to pick up, accept, transfer, or deliver video storage media containing highly sensitive data including tape backups. Backup tapes must be secured in a locked enclosure during transport and moved directly from site to site
6. All media storage devices such as hard drives, removable disk drives, diskettes, CD-ROMs, zip drives, jump drives, personal digital assistants and other storage media are required to be purged of all data when they are reassigned, salvaged, or transferred to another agency as described in the COV ITRM SEC2003-02.1 standards.