1. PURPOSE

Access to computer systems and networks owned or operated by Radford University (University) imposes certain responsibilities and obligations upon users and is granted subject to University policies and federal, state, and local laws. This policy outlines the requirements and responsibilities of users to comply with this policy and the consequences of noncompliance.

2. APPLICABILITY

This policy applies to any person assigned a Radford University account, or any person using University-owned or leased computers, networks, internet connections, and/or communication systems transmitting data, voice, or video information.

3. AUTHORITY

University policies fall within a greater hierarchy of laws, statutes and regulations. The Board of Visitors has been authorized by the Commonwealth of Virginia to govern Radford University. (See Code of Virginia §23-155.7; 23-9.2:3.)

The Board of Visitors, in the Board Bylaws, has delegated much of the authority to manage the University to the President, who serves as the agent of the Board and as the Chief Executive Officer of the University. As a part of that management, the President, in conjunction with the President’s Cabinet, will direct the development and implementation of University Policies and Procedures.

4. DEFINITIONS

User: Any person assigned a Radford University account, or any person using University-owned or leased computers, networks, internet connections, and/or communication systems transmitting data, voice, or video information.

5. POLICY

A. As a public institution of higher education in the Commonwealth of Virginia, Radford University will manage its information technology in accordance with the intent of the laws of the Commonwealth and the additional operational authority granted to the University by the
Virginia General Assembly, as set forth in Subchapter 2 of the Restructured Higher Educational Financial and Administrative Operations Act, §23-38.88 et seq. of the Code of Virginia and Chapters 824 and 829, Acts of Assembly, 2008. The Board of Visitors originally approved the University to operate under this delegated authority for information technology in the Board of Visitors Resolution dated April 23, 2009. In the Board of Visitors Resolution dated May 4, 2012, the Board authorized the President and the Vice President for Information Technology and Chief Information Officer to take all actions necessary or advisable to continue the delegated authority. Upon approval of appropriate memoranda of understanding, the President and the Vice President for Information Technology and Chief Information Officer were granted full continuation of the authority and responsibility for the management of the information technology function of the University. This delegation includes the authority to conduct these activities in accordance with industry best practices appropriately tailored for the specific circumstances of the University in lieu of Commonwealth determined specifications.

B. Access to University information systems is a privilege that may be revoked for reasons including, but not limited to, violations of this policy. Violations of this policy may be subject to disciplinary action. Violators may also be subject to prosecution under various relevant federal, state, or local laws.

C. Specific requirements and responsibilities of users for access to University information systems are as follows:

1. Users are responsible for all activity that occurs in or through their accounts and/or their computers or network enabled devices, whether personally or University owned.

2. Users must not share access to their individually assigned accounts.

3. Upon notification from the University’s IT Security Office or Technology Assistance Center (TAC) that an account has potentially been compromised, users must follow the instructions provided.

4. Users must only access information that is their own, information to which they have been given authorization to access, or public information.

5. Users with access to highly sensitive, or protected information as defined within the IT 5102 – Data Storage and Media Protection Policy must follow that policy to properly safeguard information.

6. Faculty and staff must comply with Virginia Department of Human Resource Management Policy 1.75 – Use of Electronic Communications and Social Media.

7. Software not used explicitly for academic instruction, or otherwise needed to complete assigned job responsibilities, must not be installed by users on University-owned equipment or systems.
8. Users must not remove or alter software or hardware on University-owned equipment or systems that adversely affects the security, integrity, and/or performance of the University systems and data.

9. Users must not attempt to interfere with the normal operation, integrity, validity, or the security of any University information system.

10. Users must not attempt to misappropriate or guess passwords.

11. Users must not use other computers or programs to decode passwords, access restricted system control information, or monitor restricted system or network communications.

12. Users must not engage in any activity that might be purposefully harmful to University systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to University data.

13. Users must not conduct scanning of University network connected devices or systems that has not been authorized by the Radford University IT Security Office.

14. Users must refrain from monopolizing or wasting University resources such as network bandwidth, disk storage, printer paper, etc.

15. Users must report possible violations of this policy, security violations, or security problems to the University by sending an email to abuse@radford.edu or the University’s IT Security Office at itsecurity@radford.edu.

16. Users must assist University officials with the investigation of violations of University computing policies.

17. Users must abide by all relevant federal, state and local laws governing copyrights, trademarks, licensing terms for corporate software, ownership of information, and related material.

18. Users must refrain from engaging in any illegal activities, such as software piracy, through either distribution of copyrighted software or illegal attainments of software and other copyrighted materials, including digital documents, articles, and images.

19. Users must refrain from engaging in any illegal peer-to-peer file sharing. Such activity is not only subject to federal and state penalties; it increases security risks for the University’s network. The University’s IT Security Office will actively investigate, report findings, and take necessary disciplinary action for any such activities.

20. Users must use software in compliance with all vendor requirements and agreements.

21. Users must observe the conditions of the Radford University Privacy Statement when developing web pages and web applications.

22. Users must not use University systems to view, access, display, download, print, store, or transmit obscene or pornographic material in violation of federal, state, and local laws.
23. University information systems must not be used for non-University affiliated purposes, ongoing business enterprises (other than University-approved business), partisan political purposes, or for any unauthorized mass mailings.

24. Users must not use University systems to defame, harass, or intimidate any person or group of persons.

D. Access may be revoked temporarily by the University to safeguard University resources, protect its network from systems and events that threaten or degrade operations, limit the University’s liability for damages due to violations of this policy, and investigate allegations of abuse of this policy.

6. PROCEDURES
The Division of Information Technology (DoIT) has developed specific standards, procedures, and guidelines, as appropriate, for the implementation of this policy and the management of the information technology functions of the University. These standards, procedures, and guidelines are maintained and hosted by DoIT due to the technical and sensitive nature of the information security program. Publicly accessible standards, procedures, and guidelines may be found at http://www.radford.edu/content/it/home/it-policies.html. Other internal standards, procedures, and guidelines of a sensitive nature are available upon request to appropriate and relevant parties by contacting DoIT.

7. RESPONSIBILITIES
The Vice President for Information Technology and Chief Information Officer will maintain the framework for the information security program, including updating the standards, procedures, and guidelines when necessary.

8. INTERPRETATION
The authority to interpret this policy rests with the President of the University and is generally delegated to the Vice President for Information Technology and Chief Information Officer.

9. EXCLUSIONS
None.

10. REFERENCES

Chapter 824, Virginia Acts of Assembly 2008

Chapter 829, Virginia Acts of Assembly 2008
Radford University Board of Visitors Resolution, “Approval to Continue Level II Authority”, May 4, 2012 (See Attachment E in Minutes)

Radford University Board of Visitors Resolution, “Information Technology and Procurement Operational Authority (Level II)”, April 23, 2009 (See Attachment B in Minutes)

11. APPROVAL AND REVISIONS

The President of the University and the President’s Cabinet have approval authority over this policy and all subsequent revisions.

The Acceptable Use Policy for University Computers and Information Technology Systems was initially approved by the President’s Cabinet on September 3, 2009. The policy was revised in April 26, 2011 to reflect a change in the name of DHRM policy 1.75, Use of Electronic Communications and Social Media.

The new Acceptable Use Policy for University Computers and Information Technology Systems, reformatted into the University-wide policy template, was submitted to and approved by the President’s Cabinet at the meeting held on September 10, 2014, and was signed by President Kyle.

For information, contact the Office of Policy Compliance – 540-831-6651