RADFORD UNIVERSITY

Policy Title: Acceptable Use Policy for University Computers and Information Technology Systems	**Effective Date: 9/3/2009**
Policy Number: IT-PO-1500	**Date of Last Review: 8/22/2017**
Oversight Department: Office of the Vice President for Information Technology & CIO	**Next Review Date: 8/1/2020**

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 University computer account, or any person using University-owned or leased computers, networks, internet connections, and/or communication systems transmitting data, voice, or video information.

3. DEFINITIONS

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

4. POLICY

A. 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.

B. 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 (DHRM) 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 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 *Internet 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.

C. 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.

5. 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.

6. EXCLUSIONS

None

7. APPENDICES

None

8. REFERENCES

Code of Virginia, Title 23.1, Chapter 10 (§ 23.1-1000 et seq.), "Restructured Higher Education Financial and Administrative Operations Act."

Chapter 824, Virginia Acts of Assembly 2008, "Restructured Higher Education Financial and Administrative Operations Act"

Chapter 829, Virginia Acts of Assembly 2008, "Restructured Higher Education Financial and Administrative Operations Act"

9. AUTHORITY AND INTERPRETATION

Information technology is managed under delegated operational authority granted to the University by the Virginia General Assembly, as set forth in the Restructured Higher Education Financial and Administrative Operations Act, § 23.1-1000 et seq. of the Code of Virginia, and Chapters 824 and 829, Acts of Assembly, 2008. The Board of Visitors (Board) approved the University to operate under this delegated authority in Board resolutions dated April 23, 2009, and May 4, 2012. Accordingly, 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 (CIO).

10. 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.

Effective February 1, 2017, the *Acceptable Use Policy for University Computers and Information Technology Systems* was reviewed by the oversight department and the Office of Policy Compliance. The policy was modified to conform to the new University Policy template with only minor revisions not requiring approval of the President's Cabinet.

Effective August 22, 2017, the *Acceptable Use Policy for University Computers and Information Technology Systems* was reviewed by the oversight department and the Office of Policy Compliance. Minor revisions were made that did not require approval of the President's Cabinet.

For general information concerning University policies, contact the Office of Policy Compliance – (540) 831-5794. For questions or guidance on a specific policy, contact the Oversight Department referenced in the policy.