Policy Title: Log Review & Storage	**Effective Date: 2/19/2009**
Policy Number: IT-PO-5200	**Date of Last Review: 06/26/2026**
Oversight Department: Information Technology Services	**Next Review Date: 06/26/2027**

1. Purpose

Radford University is committed to maintaining a reliable and secure technology infrastructure. Logging of system events to a centralized log host provides a method of reviewing system for activity, failures and security events. This policy provides the guidelines for managing and retention of log files as well as the routine review of log files.

2. Policy

A. All university systems should synchronize their time clocks using Network Time Protocol (NTP).
B. Where possible, log events to a centralized log server. These logs should be copied to a centralized log server in real time or as near real time as possible.
C. All system log files should be retained for at least 60 days. Log files for servers should be retained for at least 120 days.
D. Informational or debug logging should be used only for diagnostic purposes, and should be disabled upon completion of the diagnostic session.
E. System and network administrators are responsible for reviewing log files on a daily basis for critical errors and security threats.
F. The use of keystroke logging is prohibited except for IT security investigations and when approved in writing by the CIO.

3. Procedures

Procedures necessary to comply with this policy are dependent upon system capabilities and are left to the discretion of System Owners and System Administrators.

4. Definitions

Network Time Protocol (NTP) – a protocol used to synchronize the clocks of computer systems.

5. Related Information

6. Policy Background

7. Approvals and Revisions

Approved: July 14, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: 9/24/2008
Minor changes for clarification.
Approved: September 24, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: 12/18/2008
Policy renumbered to Information Technology Policy 5200 from former Information Technology Policy 110.
Approved: December 18, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: 2/19/2009
Policy revised to include the prohibition of keystroke logging.
Approved: February 19, 2009 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 2/19/2012
No changes.
Approved: February 19, 2012 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 2/11/2019
Policy reviewed during security standard review with minor wording changes for clarification. Revised with updated template.
Approved: February 19, 2019 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 2/4/2022
Policy reviewed during security standard review with minor wording changes for clarification. Revised with updated template.
Approved: February 11, 2022 by Associate Vice President for Information Technology & CIO, Ed Oakes

Reviewed: 1/27/2025
Added wording regarding informational and debug logging.

Reviewed: 06/26/2026
No changes.
Approved: June 26, 2026 by CISO Bob Burton.