COLLEGE OF WILLIAM AND MARY

INFORMATION SECURITY POLICY STATEMENT

The Information Security Policy Statement was recommended by the administration and approved by the Faculty Assembly of the College of William and Mary on 24 September 2002.

BE IT RESOLVED, That upon recommendation of the President, the Board of Visitors adopts the following *Information Security Policy Statement* for the College of William and Mary in Virginia.

This policy of the College of William & Mary views administrative data, third party proprietary information, and College information systems as critical business assets. Misuse or damage of administrative data, third party proprietary information, or College information systems may be as costly to the College as misuse or damage of physical property. College employees are responsible for the protection and proper use of College administrative data, third party proprietary information, and information systems according to the policy provisions set forth below. Please read the policy carefully before acknowledging awareness of these provisions.

1. Restricted College administrative data and third-party proprietary information (e.g., licensed software and designated portions of vendor contracts) in the custody of College staff members shall be used only for official College business and as necessary for the performance of assigned duties. Restricted College information includes student records that are confidential under the Family Educational Rights and Privacy Act (FERPA 1974, as amended), personnel records, and other data to which limited access is subject to prior administrative approval.

2. College administrative data or third-party proprietary information shall not be altered or changed in any way except as authorized in the appropriate performance of assigned duties.

3. College administrative data or third-party proprietary information shall not be divulged to anyone unless their relationship with the College as an employee, customer, vendor, or contracted temporary employee warrants disclosure and is authorized or required by law and College policy.

4. Unless publicly available, College administrative data shall only be accessed by staff members who are specifically authorized to do so.

5. College information systems shall not be used for personal economic benefit or for political advocacy. Occasional use (e.g., email, web) of College information systems for personal use is acceptable if it does not interfere with a staff member’s job performance. Any use of a staff member's private office for external paid employment is also subject to College review as specified in the College's Policy on External Paid Employment (approved by the Board of Visitors, 2 February 1996).

6. Any user IDs and passwords assigned to a staff member shall be used only by that staff member and shall not be divulged to persons not authorized by the College.

7. The College strictly prohibits illegal use of copyrighted software and materials, the storage of such software and materials on College information systems, and the transmission of such software and materials over William and Mary network facilities.

8. The College is providing staff members with access to shared resources. Staff members shall not knowingly engage in any activity harmful to the College's information systems, administrative data, or third-party proprietary information. (e.g., creating or propagating viruses, overloading networks with excessive data, instituting or promulgating chain letters, or instigating unauthorized mass postings of any type).

9. William & Mary information systems shall not be used to engage in any activity prohibited by College policies, or by state or federal law.

10. College staff members shall not circumvent or subvert any College system or network security measures. They shall not use College email services to harass or intimidate another person. They shall not send email using or impersonating someone else's user ID or password.

11. The College does not routinely inspect, monitor, or disclose electronic mail. However, electronic messages are written records and may be subject to disclosure under the Freedom of Information Act, legal process, or College review upon receipt of a credible allegation of misconduct. The College will investigate and may pursue appropriate internal or external civil or criminal proceedings when misuse of College administrative data, third party proprietary information, or College computing resources is suspected.

12. Failure to comply with any of the above stated policies may result in a staff member being disciplined or terminated from his or her position, in accordance with general employment policies and procedures that apply to respective categories of employees.

13. This policy does not affect the duties, powers and responsibilities of the Board of Visitors.

B/V approval 22 November 2002