From: The President
To: MC Communications List
Subject: Private Data Found on College Web Folder
Date: Friday, May 11, 2012 6:29:36 PM

MONTGOMERY COLLEGE
Office of the President

May 11, 2012

MEMORANDUM

To: Montgomery College Colleagues

From: Dr. DeRionne P. Pollard, President

Subject: Private Data Found on College Web Folder

In our current times, it is important that our College keep confidential data safe and secure. With this in mind, it is disappointing to have to share information that was brought to my attention yesterday evening. This memorandum is coming out now, as opposed to Monday morning, because I thought it important to share the information my senior leadership team has gathered and the initial steps taken.

A Montgomery College professor conducting a web search discovered a faculty workload report, in PDF format, that contained the Social Security numbers of full-time instructional faculty members from the 2001–2002 academic year. He reported it to his dean, who reported it to Vice President of Human Resources, Development, and Engagement Sarah Espinosa. She immediately contacted the Office of Information Technology (OIT), which took corrective action. She also contacted my office, and a subsequent call went to Professor Rick Penn, president of the Montgomery College Chapter of American Association of University Professors (AAUP).

Initial research by OIT found the report and removed it last evening; OIT also worked with Google and other search engine companies to remove the document from their caches. At this point, we do not believe anyone's data has been comprised, but we are seeking a firm to provide identity theft protection for the instructional faculty members listed in the report. More information about this will be shared as soon as possible.

The report's discovery recalls a previous incident that occurred in December 2010, in which a similar document with private data was found online. Following that discovery, OIT scanned the College website for any other documents containing private employee data, and none was found. At this time, I have charged Stephen Cain, chief of staff/chief strategy officer, with conducting a thorough review of what has happened and with taking appropriate actions with respect to any persons that are accountable. I believe an in-depth review of our operations is absolutely essential.

It is clear that our organization must do more to protect private confidential data. Past practices for handling this data may no longer be acceptable. Therefore, I will ask the Board of Trustees to consider a new policy governing data use and security. In addition, I have also

asked Dr. Cain to work collaboratively with Vice President of Information Technology and Chief Information Officer Mike Russell to develop new institutional procedures for handling confidential data. We must ensure that only those faculty and staff members who legitimately need access have access, and that our organization has a comprehensive plan for protecting confidential and private data.

As we move forward, my senior leadership team and I will work to maintain your trust. Thank you for your cooperation and assistance in the days and weeks ahead.