Notification Procedures in Case of Breach of Privacy

The University of Arkansas takes several measures to ensure the privacy of personally identifying information it collects and maintains about faculty, staff, and students.

The University Data Center hosts servers for storing sensitive data in a controlled access area. Servers are secured with firewalls, virtual private networks, data access monitoring software, and passwords, as well as other methods. The State of Arkansas Security Standards are applied to data storage and access in the University Data Center.

Access to personally identifiable information is limited to those employees with a legitimate, job-related need to know. Employees have access only to those data elements which they actually need for designated purposes, and access is controlled through an electronic desk system and other security access systems. There is regular review of those data elements to which individual employees are allowed access.

In August of 2004, the University adopted the "Employee and Student Data: Use and Security Policy," Academic Policy Series 1900.10 to address the correct use of personally identifiable information. A comprehensive policy concerning the privacy of sensitive information on the University's website is currently being reviewed.

If security is breached and personally identifying information is compromised, the University will immediately notify law enforcement officials including, as appropriate, University Police, the FBI, the U.S. Secret Service, the U.S. Postal Inspection Service and/or other law enforcement agencies.

The University will contact everyone whose identity may have been put at risk, regardless of whether personal data appears to have been accessed or extracted. It will also notify the campus community about the security breach through electronic and others means. The notification will include the following information:

-Exactly when and how did the breach occur, and when was the breach detected?
-How many individuals are affected?
-What personal information was put at risk?
-Does the University know whether any information was stolen?
-What procedures did the University follow with regard to the security breach?
-How should individuals respond if they discover fraudulent use of their personal information?
-What steps is the University taking to prevent illegal access of confidential information in the future?
-What has the University done to notify those affected?
-Who can respond to additional questions concerning this security breach?

The custodian of the data is responsible for notifying those affected by an electronic security breach. In the case of a non-electronic security breach, the office or department where the breach occurred will be responsible for notification.

June 14, 2006