



Minnesota
STATE COLLEGES
& UNIVERSITIES

OFFICE OF THE CHANCELLOR
OFFICE OF GENERAL COUNSEL

WELLS FARGO PLACE
30 7TH ST. E., SUITE 350
ST. PAUL, MN 55101-7804

ph 651.296.3905
fx 651.296.6580
www.ogc.mnscu.edu

MEMORANDUM

Date: December 14, 2006

To: Minnesota State College and University Presidents and
Chief Information Officers

From: Ken Niemi, Vice Chancellor Information Technology Services
Gail M. Olson, General Counsel

Subject: New Breach of Security of Data System Standard
Minnesota Statutes Sect. 13.055

To help individuals protect themselves against identity theft, the legislature amended the Minnesota Government Data Practices Act (MGDPA) effective August 1, 2005, to require state agencies to notify affected individuals of breaches in the security of private or confidential data about themselves. Minn. Stat. Sect. 13.055.¹ Unlike the laws of many other states that address this concern, Minnesota law broadly applies to any private or confidential data about individuals in any medium. The law details how notice must be given, the timing of the notice, and many other specifications.

Over the past several months, the Office of General Counsel, in consultation with Information Technology Services personnel of the Office of the Chancellor and campuses, has developed a detailed System Standard to assist colleges and universities in implementing a notice procedure. The Standard may be found on the IT Security Web-site at:

<http://its.mnscu.edu/security/breachnotification/index.html>

The Standard contemplates each president designating a "Lead Campus Authority" who is responsible for overseeing implementation of the Standard. This individual may be your CIO, your campus Data Practices Compliance Official (DPCO) or any high level administrator. At this time, we do not ask you to report the identity of this individual to the Office of the Chancellor, but may do so in the future.

¹ You may obtain a copy of the text at: www.revisor.leg.state.mn.us .

MnSCU Presidents and CIO's

Page 2

December 8, 2006

Additionally, given the need to provide timely notice to affected individuals, all employees should know of their responsibility to report any suspected security breach to their supervisor or manager. To assist in that regard, a sample notice for all employees is attached at the end of this memo.

Thank you for your assistance in this matter. We hope these documents will be useful. Please contact Kris Kaplan in the Office of General Counsel at 651 296-3905, or kristine.kaplan@so.mnscu.edu for additional information.

Cc: Cabinet
HR Directors Listserv

Att.

Sample Notice to Employees

Security Breach Reporting

State law requires Minnesota State Colleges and Universities to notify individuals of a breach of the security of their private or confidential data – regardless of the form of the data. Timely notice is important to counteract potential identity theft. Good faith acquisition of data by an employee, contractor or agent of MnSCU is not considered a breach so long as the data is not additionally provided to an unauthorized person.

Any employee who believes he or she is aware of an unauthorized acquisition of data, which compromises the security and classification of that data, is expected to report the incident to his or her supervisor or manager immediately. Suspected electronic breaches may also be reported to the Office of the Chancellor Information Technology at: Security@mnsu.edu or by calling 1-877-GOMNSCU (1-877-466-6728); Press 3 for Enterprise Technical Support then Press 1 for Network Support.

Thank you for your assistance in this important matter. The System Standard may be found at:

<http://its.mnsu.edu/security/breachnotification/index.html>