

College of Education Guidelines Regarding Data Security

October 22, 2009

Each employee in the College of Education is responsible for the security of university data with which they are entrusted. In order to meet this obligation, faculty and staff who collect or maintain any data concerning students, research subjects, credit cards, personnel information and the like, should be aware of the following

1. University guidelines concerning security

Managing Sensitive Data:

<http://computing.msu.edu/msd/>

Safe and Secure Computing at MSU:

<http://computing.msu.edu/secureit/>

MSU Acceptable Use:

<http://www.msu.edu/au/>

MSU PDF on Security Breaches:

http://lct.msu.edu/documents/SECURITY_BREACH_GUIDELINES_revised_July_2009.pdf

2. Additional College of Education guidelines concerning security

- Data security breaches should be reported immediately to the College computer support group
- Your NetID and password define your online identity at MSU. Guard your passwords and pass phrases as you guard your bank card PIN.
- College offices may not maintain highly sensitive data such as social security numbers on any computer connected to the internet.
- College offices may not maintain credit card numbers and instead use the MSU WebCredit system.
- Requests for access to university data and electronic personnel and financial forms are submitted, along with a “need to know rationale” to the college security officer prior to submission to MSU.
- Support staff in the College are required to enroll in a College sponsored “data security workshop” at least once every 3 years. These workshops will be announced periodically.
- Student employees must sign a confidentiality statement upon employment.
- The Assistant Dean for Budget and Operations will send an annual notice to College of Education employees addressing security guidelines.