

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor



Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members
CC: Ila Saunders, Internal Audit, MSU
FROM: Nathan Tobin, Information System Auditor
DATE: June 25, 2007
RE: Follow-up IS Audit, Montana State University Electronic Research Data Security (06DP-01)

INTRODUCTION

We presented our information system (IS) audit of electronic research data security at Montana State University (MSU) to the Legislative Audit Committee in June 2006. The report contains one recommendation, which contain two specific parts. The recommendation relates to:

- ▶ The formal designation of a responsible party to oversee the security of electronic research data.
- ▶ The implementation and enforcement of a policy that addresses the security of electronic research data.

We requested and received information from MSU personnel regarding progress toward implementation of our report recommendation. This memorandum summarizes their response.

BACKGROUND

MSU has been recognized as one of the top performing research institutions in the country. During fiscal year 2005, the MSU-Bozeman Office of Sponsored Programs administered \$98 million in grant and contract sponsored research activity. MSU-Billings administered an additional \$600,000. The research that results from this funding often produces unique and valuable data. Because this data is often stored electronically, and because academic institutions tend to be susceptible to computer instruction and data theft, we conducted an audit to determine if MSU was effectively securing electronic research data.

Follow-up Discussion

The following section summarizes the report recommendation, and the university's progress towards implementing the recommendation.

Recommendation #1

We recommend the university:

- A. Formally designate responsibility for electronic research data security; and
- B. Implement and enforce a policy to address electronic research data security requirements.

Data Quality

Our 2006 audit found that no centralized policy or guidelines existed regarding electronic research data security. Responsibility for securing research data fell to the Principal Investigators, or lead researcher, on each individual research project. We found that because of the decentralized nature of securing electronic research data, the level of security implemented varied between different Principal Investigators. In a number of instances we identified areas where security was not sufficient, resulting in vulnerabilities that could lead to the exploitation and theft of data. We recommended MSU develop a centralized policy to address the security of electronic research data and designate a party responsible for implementing and enforcing this policy.

Recommendation Status:**A. Implemented**

During the 2006 audit, we found that MSU had not implemented a policy that designated any individual or party as responsible for securing electronic research data. In December of 2006, the university adopted policy to address this recommendation. After reviewing this policy, we found Principal Investigators have been formally designated as the responsible party for securing research data. Also, each Principal Investigator must agree to read and adhere to the centralized MSU data security guidelines developed by the Information Technology Center (ITC) at MSU.

B. Partially Implemented

Since the 2006 audit, the university has implemented an electronic research data security policy designating Principal Investigators as responsible for securing data resulting from their research projects. The policy is also supported by the university's general data security guidelines. These guidelines provide specific security measures that are required to be implemented when storing research data, including maintaining current system patches and anti-virus, physically securing data storage devices, and proper storage of sensitive data. Additionally, university data stewardship guidelines are being developed and a draft has recently been issued for comment. These guidelines will further define who is responsible for securing data and the different levels of data sensitivity. University personnel project that these guidelines will be in place by summer of 2007. The university is still considering options on how to best educate and implement these policies and guidelines among the Principal Investigators.