Encryption keeps data secure
Tip of the month from Internal Audit

May 27, 2008

This is part of a continuing series of monthly tips from Ohio University’s Office of Internal Audit that address common errors, misunderstandings and control failures often found during audits. Internal Audit performs departmental and process reviews, working collaboratively with units to assess and improve controls across the university.

Normal e-mail is not a secure way to send confidential information such as security numbers, credit card numbers or other sensitive data to Payroll, Human Resources, Accounts Payable or other university offices because of the potential for the data to be viewed in transit.

E-mailing such information requires that the sender encrypt the data. The Office of Information Technology is available to discuss encryption options for university employees’ e-mail clients.

Copying the data to a disk or thumb drive also is not a secure way to share sensitive information. Many security breaches involve the loss of an unencrypted storage device, such as a thumb drive, that contains sensitive data. If you lose such a storage device with confidential data, the university may be required to report a security breach to affected individuals and certain agencies.

Practicing safe computing is the responsibility of all university employees. To discuss encryption options, contact OIT at 593-1222 or security@ohio.edu.