Sensitive data: handle with care
Tip of the month from Internal Audit
Jul 30, 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.

Our last article discussed the importance of encrypting e-mails that contain sensitive or protected information. A more basic question is: Do you really need to collect and send the information?

There are times when Social Security numbers, tax ID numbers, credit card numbers and student information must be communicated across the campus, but often this information can be obtained through more secure systems.

Ask yourself these questions before you collect, store or send sensitive data:

1. What is the business need? Is the sensitive data really necessary?
2. If you need a unique identifier, is there a more secure alternative such as employee or PID number? In some cases, first name, last name and some other nonsensitive information, such as phone number, is sufficient to identify an individual.
3. Are you using the information as originally intended? For example, if you collected a credit card number for a purchase or registration, are you sending the number to someone to use for a different purpose? This is not permissible; the card holder must authorize the additional use.

Information is one of Ohio University’s most precious resources. Make sure you use and protect information appropriately. If you are unsure of the alternatives available or would like further information, please contact the university’s Information Security Office by e-mail at security@ohio.edu.