Deans, Directors, Department Heads

We have seen an increase in the collection and storage of employee and student Social Security numbers (SSN) in departmental files. While it is important to ensure that departments have information necessary to their functions, the proliferation of such storage puts members of the Duke community at greater risk for identity theft. The Office of the Chief Information Officer has studied these concerns and has produced a paper about them. You will find it online at www.security.duke.edu/whitepapers/ssn.

In accordance with these recommendations, effective immediately, all departments should begin to phase out non-essential uses of the SSN:

- Migrate all systems using the SSN as an identifier to the Duke Unique ID by 6/30/04.
- Migrate systems or processes that use the SSN to verify a person's identity to a stronger form of authentication by 6/30/04. (The Duke Unique ID is not sufficient for authentication.)
- Discontinue the collection of Social Security numbers, except where there are legitimate and legally mandated requirements (e.g. financial aid, payroll, tax reporting, etc.), by 6/30/04.

Departments wishing to continue to use SSNs as an identifier must:

- Show compelling institutional need;
- Receive approval from the Executive Vice President and the Chief Information Officer; and
- Permit yearly audits (including server and application security) to ensure safe SSN handling.

We will be examining the practice of providing database feeds across the institution. Our expectation is that, as of 7/1/05, all payroll extracts that have not been appropriately justified will be discontinued.

The Office of the CIO will coordinate with departments regarding steps they should take to protect Social Security numbers. If you have questions regarding implementing the above policy, please contact the University IT Security Office (security@duke.edu).

Thank you for your cooperation.

Tallman Trask III
Executive Vice President

cc: Peter Lange
    Tracy Puthey
    Nancy Allen