Social Security Number Usage Policy

Version 1.0

Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

Scope

While it is important to ensure that departments have the information necessary to perform their functions, use of Social Security Numbers puts members of the Duke community at great risk for identity theft.

The Office of the Chief Information Officer studied these concerns in April 2003 and produced a paper titled "Social Security Number Use at Duke University". In accordance with the recommendations of that paper a directive was issued [1] by Dr Tallman Trask III later that year.

The current policy on the collection, storage, and use of Social Security Numbers at Duke is:

Departments wishing to collect, store, or use SSNs in any way 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

Contact the Duke University IT Security Office via email at security@duke.edu [2] to verify if your institutional group is permitted to collect, store, and/or use SSNs.

Please contact the DUHS Information Security Office for the DUHS and DM process (iso@mc.duke.edu [3]).

The University process for obtaining approval is:

1. 
The department completes a Data Classification request form (available from security@duke.edu [2]).

2. The University IT Security Office reviews the form and sends a summary or proposal to CIO for approval.

3. If approved by CIO, then submitted to EVP for approval.

4. If approved by EVP, then a signed approval document is provided to the department.

5. Internal Audit is notified that the department has executive approval to collect, store, or use SSNs, and should be audited annually.

Machines collecting, storing, or using SSNs in any way must comply with the ITSO technical standard requirements [4] for Sensitive data.