

Security Standards for Social Security Numbers

Social Security numbers (SSNs) may be used in electronic transactional systems and databases only when necessary to meet business needs. This document is a companion to the Social Security Number Policy. It provides standards for the care that needs to be taken with this sensitive data element. This document may be revised at any time in order to provide the most secure environment consistent with carrying out university business. It is posted on www.security.vt.edu as well as on www.banner.vt.edu.

- **Display of SSNs on computer terminals, screens, and reports**

Physical access to computers, screens, and printers using SSNs must be as restrictively controlled as possible. Devices not in use for extended periods of time must be password-protected, and locked or shut down. Screens must be protected from the view of unauthorized users. Printers used for reports containing SSNs must be within the physical control of authorized users, and reports retrieved quickly.

- **Security protocol required to access SSNs in electronic databases**

Systems using SSNs must use strong and complex passwords. Each user must be individually authenticated. The least privilege must be granted to users necessary to complete their duties.

- **Electronic storage of SSNs**

Systems that have been approved to store SSNs must comply with the University Information Technology Security Policy, including applying patches to maintain security, keeping operating systems up-to-date, and appointing an employee to be responsible for the system.

SSNs should be stored in as few places as required for meeting business needs, including business needs to ensure data integrity through backups.

- **Electronic transmission of SSNs**

If sent across the Internet or other open network such as unprotected wireless connections, both the authentication data and the data itself must be encrypted with strong encryption.

- **Alternate mechanisms for integrating data other than the use of the SSN**

SSNs must not be used as keys to records in active files. Elements that may be used are:

- UIDs (Generated and maintained by the Enterprise Directory)
- VT ID numbers (Generated and maintained in the Banner system)
- PIDMS (Banner internal numbers)
- Locally maintained keys that are unrelated to SSNs.

Historically important files that may have used SSNs as keys to records need not be changed. However, they must be carefully protected following these standards.

- **Obtaining permission to include the SSN in any electronic system**

Systems that need to use or store SSNs must have approval from the data trustees for SSNs; namely (a) the Vice President for Information Technology, and (b) the Vice President/Vice Provost with line responsibility for the system. Other trustees should be consulted if they have responsibilities for the individuals whose records are kept in the system. (See Policy, section 2.1).