New U.Va. SSN Policy: Short Overview

Brian Davis
IT Security & Policy
VP/CIO’s Office
3/11/08
Multi-layered Security Strategies

Hardening and Securing IT Infrastructure Program

Sensitive Data Handling Strategies

SSN Initiative

University ID / ID Card Project

Dept. System ID Change
Dept. System ID Change
Dept. System ID Change

Etc.
U.Va.’s SSN Initiative

- Comprehensive initiative to phase out use of Social Security numbers (SSNs) wherever possible
- Although SSNs must be collected for selected business functions, such as meeting Federal requirements to produce W-2 tax forms and financial aid reporting, the University will be altering other business functions to use University ID numbers in place of SSNs wherever possible
Central Effort

- New University ID cards
- New University ID numbers
- Change to ISIS Online log in
- Change to ISIS green screen look up
- Interface to allow a one-time conversion of data by reference to ISIS for student SSNs
- Changes to ongoing ISIS feeds to ensure data is mapped properly
- University ID in Integrated System
- University ID will be in new Student System
Data Classification Policy
Defines three data categories (currently known as general administrative, limited access, legally restricted, but will rename to something like low sensitivity, moderate sensitivity, high sensitivity)
States that classification is determined by legal, regulation, and contractual requirements and other considerations determined by data stewards
States that classification determines the required security protections and access authorization levels. Links to data protection standards (to be maintained outside of this policy) for each data classification.
Requires that all University data be classified
Links to relevant University policies, e.g. “Protecting Privacy Rights of Students”

Data Stewardship Policy
States general philosophy concerning management of and access to University data
Defines data management roles and data use responsibilities

SSN Policy
States that SSNs are classified as “high sensitivity” data
 Specifies limited conditions under which SSNs may be collected, used, and/or reported
 States that no new systems may be purchased or developed using SSNs as primary identifier
 Requires standard explanatory wording on all public-facing forms, online screens, and other data collection mechanisms that request SSNs.
 Links to relevant University policies, e.g. “Protecting Privacy Rights of Students”

Policy Strategy: Replace Current Administrative Data Access Policy\(^1\) with these three policies

Data Protection Standards

Data Steward List

\(^1\) http://www.itc.virginia.edu/policy/admindataaccess.html
SSN Policy: Overview

- Protection & Use of Social Security Numbers
- specifies limited conditions under which SSNs may be collected, used and/or reported
- reduces the University's risk of unauthorized exposure of SSNs by
  ▫ minimizing the amount of SSN data stored
  ▫ increasing the security of these data stores
- SSNs classified as *highly sensitive data*
Sensitive Data Handling Strategies

University Processes & Supporting Systems

- Implement clearer sensitive data use policies
- Communicate responsibilities for data protection
- Implement compliance verification processes

Ensure sensitive data requested only when essential

Ensure sensitive data provided only when essential

Ensure sensitive data stored only in highly secured devices and file cabinets

Ensure sensitive data access authorized to least # of people
SSN Policy: Implementation

• Need to get approval before using SSNs in any new way
• By July 2008, departments must identify all records and records systems within their purview that use SSNs and develop a remediation plan
• By July 2009, approved plan must be implemented
For More Information

- **SSN Initiative**
  - [http://www.virginia.edu/ssninitiative](http://www.virginia.edu/ssninitiative)
  - ssn-initiative@virginia.edu

- **Project management team**
  - Brian Davis, VP/CIO - IT Security & Policy
  - Nan Keenan, VPMB - Process Simplification
  - Valerie Larsen, College - Director, ASCIT
  - Shirley Payne, VP/CIO - IT Security & Policy

- **Cross-university core team**