

New U.Va. SSN Policy: Overview

Brian Davis

IT Security & Policy

VP/CIO's Office

2/15/08



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



U.Va.'s SSN Initiative

- The transition away from SSN use will
 - Take time, money and effort
 - Cause inconvenience and process disruption
- However, the resulting enhancement in the privacy and security of personal information the University must maintain about its students, faculty, and staff make the effort very worthwhile.



Larger Background

- Increasing security breaches and leaks
- Increasing identity theft
- Increasing national and state legislative response



Central Effort

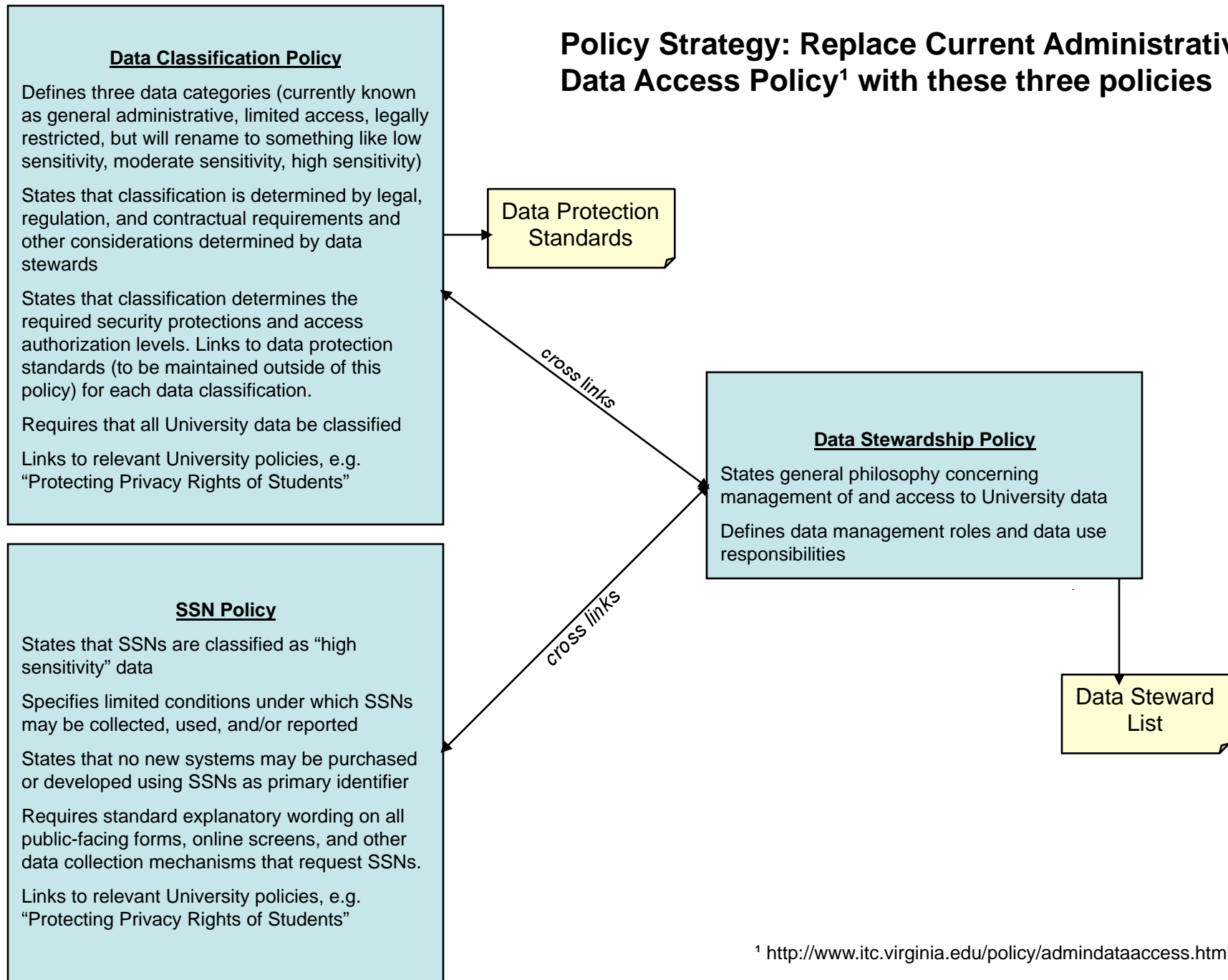
- New University ID cards
- New University ID numbers
- Change to ISIS Online log in
- Change to ISIS green screen look up
- Interface to allow a one-time conversion of data by reference to ISIS for student SSNs
- Changes to ongoing ISIS feeds to ensure data is mapped properly
- University ID in Integrated System
- University ID will be in new Student System



Policy Work

- **Administrative Data Access Policy**
 - Dates from early 90s
 - Insufficient guidance for today's environment
- **New Policy Trio**
 - **Data Classification Policy**
 - Data Protection Standards
 - **Data Stewardship Policy**
 - **SSN Policy**

Policy Strategy: Replace Current Administrative Data Access Policy¹ with these three policies



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



SSN Policy: Classification

- SSNs classified as *highly sensitive data*



SSN Policy: Do's

- handle with a high degree of security and confidentiality in compliance with policies, regulations, and laws
- collect and store only when they are essential for approved business processes or to meet legal requirements
- inform individuals who are asked to supply SSNs whether they are legally required, or may refuse, to supply the SSN

SSN Policy: Do's (cont.)

- display on online screens, reports, etc. only to those authorized to view and only when needed for an approved purpose
- authorize the fewest number of people possible to access in both electronic and non-electronic form
- maintain an accurate inventory of records that contain SSNs
- securely dispose of electronic and non-electronic records containing SSNs to minimize risk of unauthorized access



SSN Policy: Don't's

- print on identification cards or badges or include in magnetic strips or bar codes
- use as the account numbers or identifiers for individuals in new electronic or non-electronic records or record systems unless needed for an approved purpose or required by law



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



(IRS)²

- Identify and Inventory
- Remediate and Reduce
- Secure and Sustain

Find it, get rid of it, protect what you keep



Documentation

- Guidance Documents, FAQs
- Approval Forms
- Report Templates



Head's Up...

- Data Protection Standards for highly sensitive data
 - In process of drafting
 - Safeguards must be stringent given the risks, e.g.
 - Protected by customized hardware firewall
 - Annual security risk assessment
 - ...and more



For More Information

- SSN Initiative
 - <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