

**Virginia Commonwealth University**  
**Statement of Direction, Use of the Person Database**  
**Administered By: Office of Technology Services, Administrative Systems**  
**January 1, 2007**

The Person Database contains sensitive information (social security number, date of birth, VCUCard number) and other personally identifiable information for all individuals associated with the University, including employees, students and affiliates. It is essential that this information be secured and protected from accidental or unauthorized disclosure, as specified in the University's Electronic Sensitive Information and Privacy Standard.

The required method of authenticating individuals for personal access to University systems and privileges is through the real-time eDirectory, which does not require data to reside in distributed/departmental systems. All end user authentications to web-based systems that support LDAP technology are required to utilize the eDirectory protocol by August 1, 2007. (This does not apply to IT/system logon ID's used for system administration.) The sensitive data contained in the Person Database should not be used for authentication purposes after August 1, 2007, with the sole exception of physical card-swipe systems that use the magnetic stripe on the VCUCard for identification. Exceptions to this policy and/or implementation date may be requested from the University's Chief Information Officer, which must include a timeline for achieving compliance if a temporary exception is granted.

As required and with specific approval from the data owners, personally identifiable information other than the social security number, date of birth and VCUCard number may be used in departmental systems to meet University operating needs. (Use of the VCUCard number in physical card-swipe systems must also be specifically approved by the VCUCard Office.) Such usage requires compliance with the University's information security standards and policies, which are located at Information Security Management Program ([www.ts.vcu.edu/security/ismanagement.html](http://www.ts.vcu.edu/security/ismanagement.html)). The data owners are Enrollment Services, Human Resources, and the VCUCard Office. Personal financial information, including credit card numbers and bank account numbers, cannot be stored in any departmental system unless there is a documented regulatory requirement for its retention. All University Records Management policies and procedures concerning the maintenance and disposition of public records apply.

Identification of employees, students and affiliates in departmental systems (other than approved usage of the VCUCard number in physical card-swipe systems) after August 1, 2007 should be accomplished using either the individual's eID or their Banner ID number ("V" number). Both of those identifiers have been added to the Person Database in order to facilitate that transition.

On an annual basis, Administrative Systems will confirm that access previously granted to the Person Database is required and that specific information security procedures are being followed. A list of authorized users and access justifications will be provided to the University's data owners for their approval. Failure to follow information security procedures or the absence of approval by the data owners will result in the termination of access.

The current re-certification of Person Database access form is included on the next two pages for reference. Information and assistance in complying with this directive to secure sensitive information in University systems is available from:

- Robert E. Neale, Director, University Computing and Communications
- Richard S. John, Director, Administrative Systems.

Approved by:

Mark D. Willis, Chief Information Officer  
*January 22, 2007*



**CERTIFICATION OF ACCESS TO THE PERSON DATABASE**  
**As of: January 1, 2007**

**Part 2 – Individual’s Statement of Confidentiality and Compliance**

I acknowledge and understand that I have access to confidential information regarding employees, students, patients, or the public. In addition, I acknowledge and understand that I am required to reasonably comply with all applicable federal, state, and University policies, procedures and regulations or seek official exceptions to applicable policies and procedures. Therefore, except as required by law, I agree that I will not:

- Access data that is unrelated to my job duties at VCU;
- Disclose to any other person who does not have a business “need to know,” or allow any other person access to, any information related to VCU that is proprietary or confidential. Disclosure of information includes, but is not limited to, verbal discussions, FAX transmissions, electronic mail messages, voice mail communication, written documentation, “loaning” computer access codes, and/or any other transmission or sharing of data.

I understand that VCU and its employees, students, patients, or others may suffer irreparable harm by disclosure of confidential or proprietary information and that VCU may seek legal remedies available to it should such disclosure occur. I understand that failure to comply with applicable policies, procedures, and regulations may result in a loss of resources and that VCU may seek legal remedies available to it should such losses occur. Further, I understand that violations of this agreement may result in disciplinary action, up to and including, termination of my employment.

\_\_\_\_\_  
Signature, xxxxxx

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature, yyyyyy

\_\_\_\_\_  
Date

**Part 3 – Description of Usage**

Information from the Person Database is used as follows:

1. \_
2. \_
3. \_
4. \_

*Check as appropriate (“sensitive data” refers to social security number, birth date, VCUCard number):*

Yes

No

- |                          |                          |                                                                                                                                                                                                                                |
|--------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | Is sensitive data from the Person Database stored in your departmental servers/systems?                                                                                                                                        |
| <input type="checkbox"/> | <input type="checkbox"/> | Is non-sensitive data from the Person Database stored in your departmental servers/systems?                                                                                                                                    |
| <input type="checkbox"/> | <input type="checkbox"/> | Can your departmental staff access sensitive data from the Person Database?                                                                                                                                                    |
| <input type="checkbox"/> | <input type="checkbox"/> | Can other users access sensitive data from the Person Database in your systems?<br>Please identify: _____                                                                                                                      |
| <input type="checkbox"/> | <input type="checkbox"/> | Do you provide sensitive data from the Person Database to other departments?<br>Please identify: _____                                                                                                                         |
| <input type="checkbox"/> | <input type="checkbox"/> | Do you provide sensitive data from the Person Database to any external entity?<br>Please identify (will require additional follow-up, and compliance with the standard for Business Associates and Contracted Sites):<br>_____ |