



## Top 10 Best Practices For Data Handling

- 1. *Systems should not include restricted information unless it's absolutely necessary.*** Certain types of data are considered to be restricted. These data elements are often protected by law, or sometimes by University policy. Examples of such restricted data elements include Social Security Number, ethnicity, date of birth and financial information such as credit card number or bank account number. (*Data Proprietor*)\*
- 2. *Computers, whether desktops, laptops or servers, that house restricted information, should be administered by a professional system administrator.*** It should be secured in accordance with guidelines set out by Systems and Network Security Office. (*Data Custodian*)  
<http://socrates.2001/avco/staff/confidentiality.html>
- 3. *Restricted data elements as outlined above should never be used as the "key" to a system.*** For example, if you are maintaining a listing of personnel or students, you should never select Social Security Number to be the key field. (*Data Custodian*)
- 4. *It is important not to maintain actual data in a test or development environment, rather, "mask" the restricted data such as Social Security Number with dummy information.*** In many environments, applications developers maintain a working copy of their system that is used to test changes. This is often referred to as a test or development environment. Often, the security on the computer or server that houses the test environment is not as stringent as that on the computer that runs the actual system. Access is also more open on the test or development environment. For example, a programmer may be denied access to certain sensitive data elements in an actual system, but may have complete access to the development system. (*Data Proprietor - Data Custodian*)
- 5. *Exercise great caution when deciding to download restricted data from a database system (whether maintained in your department or at the central campus) to your laptop or desktop.*** Generally systems administrators take great care in securing servers that house this data, and your personal computer may be less secure. (*User*)
- 6. *Do not email restricted data, either in the body of an email or as an attachment.*** Email is not a secure form of communication. Additionally, the recipient of your email may have a less than secure computer or may elect to forward the information to another person that you did not intend to receive this information. (*User*)
- 7. *Remember the common-sense rules about your computer if it has access to restricted data:***
  - Your computer should be restricted with a solid password or pass phrase, not shared or published. <http://bilink.berkeley.edu:10000/bilink/guide.html> or [http://www.net.berkeley.edu/faq/good\\_pw.shtml](http://www.net.berkeley.edu/faq/good_pw.shtml)
  - When your computer is not in use, it should be locked with a screensaver or logged off.
  - When you print restricted data, pick it up right away from your printer and shred the paper when you're finished with it.
  - Use shared computer accounts wisely – remember that if you have a shared account with multiple users, the data is available to all those users and if it is compromised, you don't have much of an audit trail. (*User*)
- 8. *When designing a local system that includes data elements that might be utilized in other systems, consider data integration issues.*** Define your data elements so that they are consistent with other data elements on campus. Additionally, consider including elements that will make it possible for your system to integrate with other systems on campus without using restricted elements to connect the systems. (*Data Proprietor - Data Custodian*)
- 9. *Publish and maintain an up-to-date data dictionary.*** A data dictionary will ensure that users of your data will interpret the information in the way that it was intended. Otherwise,

users may have to guess at the meaning of a particular data element or the allowed values in the data element. (*Data Proprietor - Data Custodian*)

10. **Maintain Appropriate Physical Security** - In addition to the above, when a computer contains restricted data, it should be have an appropriate degree of physical security. Servers housing secure data should always be kept in a locked server room. They frequently hold backup tapes that can easily be stolen. Take special care with a laptop that includes restricted data, in the even of theft, not only will you lose your laptop, but your sensitive data will be compromised. (*Data Proprietor - Data Custodian - User*)