



**OIT 61.002:  
Data Privacy and Ownership**

**Responsible Executive:** Chief Information Officer (CIO)  
**Responsible Office:** Office of Information Technology  
**Related Policy:** 60.201  
**Approved-On Date:** May 25, 2006  
**Effective Date:** July 25, 2006  
**Revision Date:** December 17, 2009

### **Policy Statement**

Norfolk State University is committed to the responsible use of data/information provided to or collected electronically by the University. This pertains to both personal and organizational data from and about students, faculty, staff, business partners as well as other individuals and activities. NSU will properly and effectively maintain such data in accordance with relevant federal and state laws, regulations, and similar mandates. This policy applies to all information/data maintained electronically.

### **Purpose**

This policy is intended to ensure that each member of the University community fully understands that safeguarding electronic data/information is the responsibility of every individual. Furthermore, every member of the Norfolk State University community should know data are valuable assets. A benefit the university can provide the community is to ensure electronic data can be shared effectively while used with care. This benefit is diminished whenever data is misused, misinterpreted, or access to it is unnecessarily restricted. Finally, users must also know that data that is considered sensitive or restricted must be adequately protected and never disclosed without proper authorization.

### **Procedures**

1. This policy applies to NSU faculty, staff and students and other individuals and entities supporting or visiting the University. This policy governs the privacy, security, and confidentiality of University data, especially highly sensitive data, and the responsibilities of individuals and institutional units for using University data.
2. University Data is any data required to conduct University business and operations. For the purpose of this policy, University data is generally divided into three categories: public use data; internal use only data; and, highly sensitive data.
  - a. Public use data is generally intended for public use. An example of this category of data is the University's on-line directory.

- b. Internal use only data is that data which is generally not made available to parties outside the University community. An example of this type of data is minutes from non-confidential meetings which are considered to be for internal use only and therefore not routinely disclosed to outside individuals or organizations. This category of data may be released to outside parties but such requests would normally be reviewed by a University executive and in some cases by the Office of Counsel as well. Unauthorized distribution of this data to external sources is considered a misuse in situations even an abuse.
  - c. Highly sensitive data is that data which is prescribed in contractual and/or legal specifications and/or specified in state and federal law as information that must be protected. Among the types of data included in this category are individual financial records, social security numbers, personal and/or business credit card information, and proprietary data protected by law or international agreement. When possible and reasonable, highly sensitive data should be electronically encrypted for transmission as well as storage.
3. The responsible use of personal and organization information requires that the University respect individual privacy and the privacy of those organizations with which the University conducts business and other affairs. In particular, the University will do all that it can, within reason, to protect against identity theft and other forms of unauthorized use of data. Furthermore, the University will comply with all laws and government regulations in the collection, use, storage, display, distribution, and disposal of such information.
  4. Authorized uses of sensitive data are limited to those which are necessary to meet legal and regulatory requirements; facilitate access to services, transactions, facilities and information; and, those that support efficient academic and administrative processes.
  5. Access to information will be limited to the individual whose information is produced or displayed; officials and agents of the University with authorized access based upon legitimate academic or business interest needs to know; an organization or person authorized by the individual to receive their information; a legally authorized government entity or representative or other circumstances in which the University is legally compelled to provide information; or, to other individuals or entities, as allowed by law, for purposes judged to be appropriate or necessary for the reasonable conduct of University operations or business.
  6. Safeguarding social security numbers (SSN) is the responsibility of everyone at Norfolk State University. SSNs are too often misused and this can frequently result in identify theft. Because of this, SSNs must not be posted in any manner, electronically or otherwise, nor should they be printed on any cards that are required to access University services. Personnel should not be required to transmit SSNs via the Internet unless it can be assured it is performed in a safe and secure manner through the use of an approved form of encryption technology.

7. Much of the University's financial electronic data is contained in the IFAS financial information system. Data ownership is with the Division of Business and Finance. The Office of Information Technology will coordinate with the data owner and users to help assure effective data privacy is well maintained.
8. Much of the University's student electronic data is contained in the Datatel Colleague information system. Data ownership is shared between the Divisions of Academic Affairs, Student Affairs, and Business & Finance, and, Enrollment Management. The Office of Information Technology will coordinate with the data owners and users to help assure effective data privacy is well maintained.
9. Each University department and activity is responsible for reviewing and monitoring internal procedures, reports, and documents to assure compliance with this policy. This responsibility includes providing training and control systems for the responsible use of electronic data that is accessible to members of the University community as they perform their work related tasks and assignments.
10. The University leadership expects that every member of the University community will exercise both caution and care in making their personal data available as well as that of other individuals, the University, and/or activities and organizations supporting the University.
11. University departments/activities and individuals operating websites designed to collect personal and/or organizational information must provide a link from their websites to this electronic data privacy policy. They must also inform website users about any persons or entities with whom they may share information that is collected online.