Title: Data Management

Purpose: UNC Asheville is critically dependent on its computer systems and the large quantities of information within these systems. Data ownership, access procedures and standards followed by sound procedures are necessary for the protection of University information. The formalization of data management provides the framework upon which the necessary standards and procedures for access to those University assets are governed and protected.

At UNCA the principles of data management include:

- A clear system of file ownership with designated, accountable officers.
- Criteria for granting access privileges to University information both internal and external as defined by federal and state legislation.
- Written guidelines for determining how access to data will be granted and periodic review of the actual levels of access against what the policies state.

Scope: These data management and access procedures apply primarily to all centrally managed data supported by Information Technology Services under the jurisdiction of the Director ITS Administrative Information Systems.

Creators or managers of distributive and/or departmental systems developed and administered by University departments are responsible for the security and proper use of data under their stewardship.

Policy: Each Vice Chancellor will appoint a Data Manager for each of the information systems within their area. These data managers should be responsible for distributive and/or departmental systems in addition to departmental components of centrally managed systems. Normally, the Director of an office should be appointed as Data File Manager of the information system in their respective area.

The Data Managers are the functional leaders of the Administrative Information Systems. This group meets monthly and guides application development, testing, and upgrade schedule. When security and access concerns need to be discussed, the Director of Administrative Information Systems asks to be put on the agenda for the monthly meeting and leads those discussions.

This policy strictly prohibits the sharing of user names and/or passwords in order to access data.
Definitions:

Information Technology Security Officer is a person or persons designated by the UNC Asheville CIO who can verify that accounts are set up in accordance with the data manager's directives (Richard White and Robin Daugherty).

Data File Manager Responsibilities

1. Assume responsibility for system data flow and work collaboratively with Information Technology Services in designing criteria for new systems or major enhancements.
2. Approve or deny requests for access to data under their jurisdiction.
   2.1. Access to data will typically be limited to employees of the University but with the approval of the appropriate Data Manager may on occasion be granted to a volunteer supporting a University unit.
   2.1.1. Authorization for access by employees requires:
   2.1.2. A written request from the director or manager of the unit;
   2.1.3. The employee’s acceptance of University policies and procedures related to accessing University computers, networks, and data evinced by the employee’s completion of Appendix A (forwarded to an Information Technology Security Officer upon completion).
   2.2. Limited, fixed-term authorization for access by volunteers requires:
   2.2.1. A written request from the director or manager of the unit;
   2.2.2. Authorization for volunteers will typically be limited to 6 months;
   2.2.3. Signed acceptance by a unit employee or the director/manager accepting responsibility for the actions of the volunteer with respect to the relevant data;
   2.2.4. Approval by the appropriate Vice Chancellor;
   2.2.5. The volunteer’s acceptance of University policies and procedures related to accessing University computers, networks, and data evinced by the volunteer’s completion of Appendix B (forwarded to an Information Technology Security Officer upon completion).
3. Assume responsibility for data timeliness and accuracy.
4. Coordinate use of the information system by other University offices and resolve problems associated with definitions, timing, changes, and accessibility.
5. Approve maintenance and enhancement requirements including coordination of changes required by other users.
6. Provide staff with opportunities to enhance their knowledge of data maintenance and information retrieval.

Approved on: 10/7/2008
Next review: 10/7/2010
I have read the University’s Computing & Network Usage policy and agree to follow University policies and procedures with respect to computing and network use. In particular, I acknowledge the following:

A. The University may monitor my use of computing equipment and its networks and systems for the following purposes:
   a. To ensure the security and operating performance of its systems and networks
   b. To enforce University policies.
B. I have no expectation of privacy in the material sent or received over the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur.
C. All material prepared and utilized for work purposes and posted to or sent over University computing and other telecommunicating equipment, systems or networks must be accurate and must correctly identify the creator and receiver of such.
D. I will not use user names or passwords provided by other employees or volunteers nor will I offer my user name or password to others. Passwords may NOT be shared.

Employee name: _____________________________ (please print)
Employee signature: __________________________
Date: ________________

Please forward to an Information Technology Security Officer upon completion.
The University of North Carolina Asheville
Computing & Network Usage Agreement -- Volunteers

University Unit: ______________________________________________

Volunteer Information

Name: _____________________________________________ (please print)

Address: ___________________________________

___________________________________

Phone #: _____________________

Email:   _____________________

In the interest of offering my voluntary efforts in support of the University of North Carolina Asheville, I have read the University’s Computing & Network Usage policy and agree to follow University policies and procedures with respect to computing and network use. The University has drawn my attention to the following in particular:

A. The University may monitor my use of computing equipment and its networks and systems for the following purposes:
   a. To ensure the security and operating performance of its systems and networks
   b. To enforce University policies.
B. I have no expectation of privacy in the material sent or received over the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above.
C. All material prepared and utilized for work purposes and posted to or sent over University computing and other telecommunicating equipment, systems or networks must be accurate and must correctly identify the creator and receiver of such.
D. I will not use user names or passwords provided by other employees or volunteers nor will I offer my user name or password to others. Passwords may NOT be shared.
E. I will treat all information on University systems or in University databases as confidential.

Volunteer signature: _________________________________________

Date: __________________
Access required:

<table>
<thead>
<tr>
<th>TYPE (please check)</th>
<th>BRIEF JUSTIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>OnePort</td>
<td></td>
</tr>
<tr>
<td>Banner</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

Start Date: __________________________

Expiration Date (no more than 6 months): ______________________________

Unit director/manager name: __________________________________________ (please print)

Unit director/manager signature: _______________________________________

Date: _____________________________

Vice Chancellor name: _______________________________________________ (please print)

Vice Chancellor signature: ___________________________________________

Date: _____________________________

Please forward to an Information Technology Security Officer upon completion.