Policies and Procedures

Title: Computing and Network Use - Faculty, Staff, Contract, Non-agency Personnel, Volunteers, Vendors, and Guests

Purpose: This policy states the obligations and rules that faculty, staff, contract, non-agency personnel, volunteers, vendors, or guests must follow as a condition of their being granted access to computing, Email, and networks at The University of North Carolina Asheville.

Scope: This policy applies to all University faculty and staff, and to contract, non-agency personnel, volunteers, vendors, or guests. Faculty and staff will complete Attachment A at the time of employment. University employees who do not currently have a signed copy of Attachment A in their University personnel file will be asked to complete the form in order to retain access to University computers, networks, and systems. Contract, non-agency personnel, volunteers, vendors, or guests whose work benefits the University and requires access to University computing, networks, or systems will be required to sign Appendix B during the process of applying for access to University computing, networks, or system. This will then be maintained by ITS in paper format until suitable digital storage is developed.

Policy:

INTRODUCTION

The University of North Carolina Asheville’s (hereinafter "University") computing and telecommunications networks, computing equipment and computing resources are owned by the University and are provided to support the academic and administrative functions of the University. The use of this equipment and technologies is governed by federal and state law, and University policies and procedures. Additional rules and regulations may be adopted by various divisions and departments to meet specific administrative or academic needs. Any adopted requirements must be in compliance with applicable federal and state laws, and this policy.

I. REGULATORY LIMITATIONS

A. The University may monitor the 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. The University reserves the right to limit or deny access when federal or state laws or University policies are violated or where University contractual obligations or University operations may be impeded.
C. Employees, contract, non-agency personnel, volunteers, vendors, or guests 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.
D. 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.

E. User names and passwords enabling access to University computers, ITS networks, and ITS systems are for the exclusive use of the authorized employee, contract, non-agency personnel, volunteer, vendors, or guest. Passwords may NOT be shared.

II. PERMISSIBLE USE

Employees, contract, non-agency personnel, volunteers, vendors, or guests granted access to University computing technologies are expected to follow this policy and any related University rules, regulations and procedures in the use of computing equipment, systems and networks.

A. The use is lawful under federal or state law including those on copyright and trademark.
B. The use is not prohibited by Board of Governors, University or institutional policies.
C. The use does not overload the University computing equipment or systems, or otherwise harm or negatively impact the system's performance.
D. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).
E. The use does not state or imply University sponsorship or endorsement.
F. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.

III. VIOLATION OF POLICY

A. Any violation of this policy is "misconduct" under EPA policies (faculty and EPA non-faculty) and "unacceptable personal conduct" under SPA policies.
   a. Sanctions for violation of this policy may include one or more of the following: a revocation of access privileges; a written warning or written reprimand; demotion; suspension without pay; dismissal; or prosecution for criminal violations.
B. Any violation of this policy by a contract, non-agency personnel, volunteers, vendors, or guests will result in considering the following steps:
   a. Removal of permissions to access University computing and networking resources;
   b. Eliminating the University’s relationship with the contract, non-agency personnel, volunteer, vendor, or guest;
   c. Criminal proceedings.

IV. APPLICATION OF PUBLIC RECORDS LAW

All information created or received for work purposes and contained in University computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records Law applies. This information may be purged or destroyed only in accordance with the University records retention schedule and State Division of Archives regulations.

V. CONTRACT, NON-AGENCY PERSONNEL, VOLUNTEER, VENDOR, AND GUEST ACCOUNTS

UNC Asheville department heads may request computer and network accounts for contract, non-agency personnel, volunteers, vendors, or guests.
Accounts will typically be limited to employees of the University. On occasion, however, an account may be granted to a contractor, non-agency personnel, volunteer, vendor, or guest supporting a University unit, provided the supervising Department Head receives Vice Chancellor approval.

Limited, fixed-term authorization for access by contract, non-agency personnel, volunteers, vendors, or guests requires:

- A written request from the director or manager of the unit;
- Such authorization will typically be limited to a maximum of 6 months;
- Signed acceptance by a unit employee or the director/manager accepting responsibility for the actions of the contract, non-agency personnel, volunteers, vendors, or guests;
- Approval by the appropriate Vice Chancellor;
- The contract, non-agency personnel, volunteers, vendors, or guest’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).

It is the responsibility of the department head to notify ITS when the account should be deactivated if this occurs before the expiration date.

VI. 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. Current Information Technology Security Officers are Richard White and Robin Daugherty.

Approved on: 10/24/08
Next review: 10/24/10
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 Human Resources personnel file upon completion.
The University of North Carolina Asheville
Computing & Network Usage Agreement -- Contract, Non-Agency Personnel, Volunteers, Vendors, and Guests

University Unit: ____________________________________________________________

Applicant Information

Name: ____________________________________________________________ (please print)

Address: ____________________________________________________________

________________________________________________________________________

Category: □ Contract, Non-Agency Personnel
           □ Volunteer
           □ Vendor Vendor name: ____________________________
           □ Guest

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.

Applicant 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.