End User Computer Agreement

Policy Number: PSU-NK-ITS-000
Date: July 15, 2008
Page Count: 2

The use of the specified computer equipment is granted to the undersigned only. Each authorized user must select a level of access and responsibility for this system by choosing either the System User or the Enhanced System User level of access. Please check one.

_____ System User Responsibilities:
1. Read and agree to abide by University [http://guru.psu.edu/policies/AD20.html] & Campus [http://nk.psu.edu/StudentServices/IT/10453.htm] IT Policies and all related and referenced policies, as well as any subsequent revisions, amendments, or newly implemented policies.
2. Agree not to share account ID or password information.
3. Back up important user files.
4. Comply with all software license agreements governing installed software. (Please consult with the campus IT staff with questions or concerns.)
5. Ensure physical security of the computer at all times. (This is especially significant for laptop computers.)
6. Agree not to alter system hardware, software, or network configuration without the assistance and approval of campus IT support staff.

_____ Enhanced System User Responsibilities:
1. Abide by the System User responsibilities set forth in items 1-5 above.
2. Reconfigure original hardware and software as necessary to support the mission of the University, and, in doing so, assume responsibility for compliance with all governing policies.
3. Provide user access control to the software and data on the system.
4. Use the assigned IP address as listed below. (Use of another address is prohibited while on the campus network. Violators will be subject to removal from the campus data network.)
5. Assume sole responsibility and accountability for the system’s operation, any software installed, and its interaction with the campus and university data network.
6. Agree to periodic inspection of the assigned unit by the campus IT department to ensure compliance with University policy and software copyright laws.
7. Maintain and locate all properly executed agreements for installed software close to said system and readily available for audit to ensure compliance with terms of issuance. (A software breach will result in the system’s removal from the campus data network, and, if necessary, contacting the appropriate authorities.)
8. Agree to disconnect from the campus data network should any network or security issues arise concerning this system, including suspected virus activity or any network security bypass, until the issues are resolved.

9. Agree not to alter the computer in any way that will prevent the IT department from remotely updating/patching the operating system and its applications as well as scanning for vulnerabilities, viruses, and personally identifiable information (PII).

By signing, I agree to abide by the above policy with the system referenced below:

User’s Signature: _________________________________________
Date: _____________________________

By signing, I approve the above request and have assigned an IP address:

NK ITS Staff Signature: _________________________________
Date: _____________________________

To be completed by the requesting user and IT Department

<table>
<thead>
<tr>
<th>PSU Access ID</th>
<th>System MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSU ID #</td>
<td>IP Address (or DHCP)</td>
</tr>
<tr>
<td>System Location</td>
<td>Subnet Mask</td>
</tr>
<tr>
<td>System Type/Model</td>
<td>Gateway Address</td>
</tr>
<tr>
<td>System Serial Number</td>
<td>DNS Server Addresses</td>
</tr>
</tbody>
</table>

POLICY HISTORY:
9/17/2014 – Updated #1 in System User section to reference the newly created campus policies
8/03/2013 – Item #9 was added under Enhanced System User Responsibilities
8/23/2012 – Document was reformatted to match new format of other policies
11/20/2012 – Updated the New Kensington Data Network definition