Policy for Locally Administered Computers

To maintain a secure computing environment in the College of Engineering, the College requires that all computers be managed to conform to the University’s Network Citizenship Policy (http://cio.uiowa.edu/policy/NetworkCitizenship.shtml). You will be held accountable for compliance with that policy and the items listed below. You may be audited periodically to verify compliance.

Administrators of computers that are locally administered must:

1. Follow these baseline security standards for securing network-attached devices. Key vulnerabilities will change over time as new threats and risks emerge. Security standards will evolve in the same manner.

   **Updates**: Keep all software (operating systems and applications) up to date to the extent possible (i.e., within compatibility and certification constraints). Configure devices to install security updates automatically, or perform the operation manually on a frequent, regular basis. Only use operating systems and applications that are actively supported. Unsupported software or software that does not have recent security updates should not be directly connected to the ECN.

   **Anti-virus**: Install anti-virus software on all eligible devices, and make certain the virus detection signatures are updated daily. Configure the software to scan all incoming files.

   **Administrator passwords**: Configure accounts with high-level system access (e.g., administrator or root) to have strong passwords that are changed regularly, consistent with the Engineering password policy (http://www.engineering.uiowa.edu/ecs/it-policies/passwords-what-you-need-know).

   **Firewall**: Configure and activate firewall to block unneeded connections before connecting to ECN.

   **Support**: Know who provides technical support for the computers you use. Register all systems that store Level III sensitive data with the ITS Security Office.

   **Best practices**: Review and implement security best practices appropriate for the device in question. A collection of resources and documentation for best practices is available at the IT Security website (http://itsecurity.uiowa.edu).

2. Cooperate with the University of Iowa Information Technology Security Office (it-security@uiowa.edu or 319-335-6332) to resolve security problems identified with any systems you are responsible for.

3. Allow vulnerability scans on your computer(s) and resolve issues identified by the scans.

4. Immediately report compromises and other security incidents to the Information Technology Security Office (use the web form at http://itsecurity.uiowa.edu/incidents/incident-form.shtml or call 319-335-6332) or report it to Engineering Computer Support at 319-335-5751.

5. Comply with the individual responsibilities stated in Section IV of the University’s Acceptable Use Policy for Information Technology Resources (http://www.uiowa.edu/~our/opmanual/ii/19.htm).

6. At the end of the computer’s life or usefulness, it must be returned to Engineering Computer Services.

*Updated 3/2014*