Standards for Managing and Securing University-owned Endpoint Computing Assets

Computing systems, whether traditional desktop machines, or hand-held devices, form the backbone of University administrative, teaching, and research activity. These assets represent a substantial financial investment, contain critical and sensitive business, academic, and research information, and are essential to University operations. The loss of these assets would present the campus with serious consequences ranging from disruption of service to significant financial, administrative, and legal sanctions.

Therefore it is incumbent on the University to actively manage these assets to:

1. Secure them against loss, damage, or theft, and
2. Assure their appropriate and reliable use.

To accomplish those objectives:

- All institutionally-owned endpoint computing devices will be actively managed[1].
- Employees will assure that a standard set of tools and procedures will be applied to these devices to facilitate their management[2].
- These devices will comply with existing University technology standards governing network connectivity and security[3].
- The University, at its discretion, may allow connection of unmanaged devices to its network, subject to such controls as deemed necessary to secure its assets.

---

[1] "Actively managed" refers to the practice of configuring and monitoring the device to safeguard the device itself, as well as any stored data, and the device's role in the relevant business, academic, or research process.

[2] Please, see the accompanying Procedures for Managing and Securing University-owned Endpoint Computing Assets(currently under development).

[3] http://www.albany.edu/its/policies_security_and_privacy.htm