**Use of Dell Kbox for Desktop Patch and Change Management**

One of the most common routes for hacker attacks on the privacy of our information is through desktop and laptop computers lacking in the latest software security patches. Another primary route for attack is when changes are made to a computer’s configuration (e.g. software additions or upgrades). In order to protect the campus from compromise of our computer systems and information, all campus computers and servers will thus receive software updates by no later than the end of spring semester to ensure they are always current with the latest security patches and malware protection,

To accomplish this proactive protection of our computers, we will utilize an institutional “systems management appliance” (the Dell/Kace Kbox) that automates both patch and change management for all computers campus-wide. Use of the Kbox appliance was initiated several years ago at Sacramento State within the College of Business Administration and is in use at hundreds of institutions nation-wide, including at Humboldt State. Complete information on the advantages of this appliance can be found at [www.kace.com](http://www.kace.com).

This approach to desktop management has many advantages, including:

* The campus can approach 100% assurance that all computers and servers have the latest protection from attacks on information security.
* Automated management of computer patching and software changes across the network greatly reduces the amount of manual management of campus desktop computers, both dramatically reducing labor and significantly reducing the potential for compromise of information privacy when IT staff (either local or central) manually work on individual computers.
* The Dell appliance is highly intelligent, allowing for creation of distinct groupings to flexibly meet differing needs (e.g. one patch level for one college and another for a different college with different needs). The system also allows for user control of when certain patching or software updates occur (e.g. options to delay actions to a more convenient time).
* The same appliance allows automation and enhancement of many other aspects of desktop and laptop maintenance, including enhanced browser security, automated software distribution and updates, broadcast alerts to computers, power management, device inventory, and computer maintenance dashboards.

Patch and change management, as well as other functions of the Kbox appliance, are handled with little intrusion or inconvenience to users. The appliance itself is housed in the campus Data Center in AIRC and a very small software application is loaded on each campus computer (about 50% of existing campus computers already have this installed).

The primary intention of use of Kbox is to enhance computer privacy. It provides no information that is not already available about campus computers - it simply provides that information in a far less labor intensive and more reportable manner. Computer content on personal computers is not accessible by the Kbox, plus release of any individual information gathered by the Kbox about individual computers is both strictly prohibited and subject to close control and monitoring by our Information Security Officer. In addition, use of the Kbox greatly improves physical privacy by obviating hundreds of individual visits to faculty/staff offices by IT staff members, eliminating most of the opportunity that now exists for compromise of individual privacy during computer maintenance.