UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

RALPH J. HEXTER
Provost and Executive Vice Chancellor

OFFICE OF THE PROVOST AND EXECUTIVE VICE CHANCELLOR
ONE SHIELDS AVENUE
DAVIS, CA 95616
TEL: (530) 752-4964
FAX: (530) 752-2400
INTERNET: http://provost.ucdavis.edu

December 16, 2015

COUNCIL OF DEANS AND VICE CHANCELLORS
DEPARTMENT CHAIRS

RE: Campuswide Implementation of BigFix to Improve Cyber Security

Dear Colleagues:

The University of California is responsible for the stewardship of a vast amount of electronic information—including protected personal and health information, and highly valuable original research—that is used to conduct the University's academic and business functions. As stated in the UCOP Information Security Policy (IS-3): "Without the implementation of appropriate controls and security measures, these assets are subject to potential damage or compromise to confidentiality or privacy, and the activities of the University are subject to interruption." In light of the recent attack at the UCLA Health System, there is renewed and enhanced focus on cyber security by the Regents, President Napolitano, and university chancellors. The Chancellor has designated me as the UC Davis Campus Cybersecurity Responsible Executive.

In order to assist the Information Technology and Information Security professionals on campus to secure the university's information assets, in 2016 we will be investing in a campuswide endpoint protection solution called BigFix. BigFix is software that enables system administrators to centrally apply updates, patches, security upgrades, and software applications to participating individual desktop and laptop computers ("endpoints"). BigFix is limited to endpoint management, and does not monitor network traffic or other computer activity. BigFix has been widely adopted by University of California campuses, including UC Berkeley, UC San Francisco, UC Irvine, and UC Santa Cruz. BigFix has been in use in the majority of academic and administrative departments at UC Davis for several years, and is currently installed on more than 16,000 UC Davis work stations and laptops.

BigFix offers many benefits:

- **For IT professionals:** BigFix allows an IT person, with appropriate permission granted by faculty or staff, to apply patches and perform other maintenance on multiple computers simultaneously. Most computers connected to the campus Active Directory already have some form of management software; installing BigFix will improve our capabilities and ensure a consistent level of quality.
- **For Faculty who manage their own computers:** Computers will be better protected without the need to worry about keeping up with the latest updates to Operating System and application software. Protected computers will be compliant with cyber security

requirements. And faculty will have the self-service ability to download and install certain software in compliance with license agreements.

- **For everyone:** BigFix allows the campus to respond very quickly in the event of a threat or cyber-attack to identify and protect computers that may be vulnerable, protecting valuable information assets, and saving time, money, and UC Davis's reputation. (Refer to Stanford University case example http://news.stanford.edu/news/2005/september14/bigfix-091405.html.)

Because of the significant benefits of this tool, we have determined that it should be centrally funded and deployed as a campuswide solution. Starting in 2016, we will require (and fund) the installation of BigFix on all campus-owned or -managed endpoints. Doing this will provide significant benefits to the campus, including ensuring that endpoints have up-to-date patches and anti-virus protection, and allowing IT professionals to proactively identify security vulnerabilities and respond effectively to cyber-attacks.

This initiative is supported by the Chief Information Officer and Vice Provost for Information and Educational Technology, the Chief Information Security Officer, the Dean's Technology Council, the Academic Senate, and a broad coalition of IT professionals on campus.

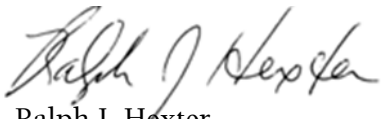
The Office of the CIO-VP is currently convening a cross-functional team to plan for the effective implementation of this solution beginning in January 2016. The plan will include a self-service website where faculty can learn more about BigFix and opt to install it on computers that are not currently managed by IT staff or request assistance in the installation process.

Deans and department heads carry a significant responsibility for helping to establish and enforce information security best practices for the systems and data they oversee. Please ensure that your IT professionals are aware of the BigFix implementation and are working on plans to get it installed as soon as possible on all workstations connected to the campus network and used by faculty, staff, and student employees.

Questions about the BigFix initiative can be addressed first to your local Information Technology support staff; or call or email IT Express (ithelp@ucdavis.edu; 530-754-HELP), which will direct inquiries to the appropriate resource. Requests for exemptions should be directed to the CISO using the standard exemption process.

Participation in this initiative will help keep UC Davis information assets as secure as possible and in compliance with laws and regulations pertaining to the protection of personal and health information. Thank you for your support in implementing this new endpoint protection solution.

Sincerely,



Ralph J. Hexter
Provost and Executive Vice Chancellor

c: Chancellor Katehi