

**SPECIAL REPORT**  
of the  
**UNIVERSITY COMPUTER AND ELECTRONIC COMMUNICATIONS  
COMMITTEE**  
concerning  
**SECURITY OF COMPUTING AND TECHNICAL EQUIPMENT  
IN ACADEMIC SPACES**

Presented at the  
660<sup>th</sup> Regular Meeting of the Faculty Senate  
March 15, 2007

**COMMITTEE MEMBERSHIP**

**Jennifer Parenti, Chair**

**Emily Alling**

**Thomas Blake**

**Steven Brewer**

**MJ Canavan**

**Leda Cooks**

**John Dubach**

**Andrew Effrat**

**Murray Eisenberg**

**Benjamin Hood**

**Pat Kochin**

**Joseph Kunkel**

**Robert Levin**

**Ernest May**

**Bruce McCandless**

**Timothy Randhir**

**Randy Sailer**

**Norman Sims**

**Howard Stidham**

**Nikki Stoia**

**Russell Tessier**

**David Toomey**

**Donna Zucker**

## **Executive summary**

Departments, faculty and students of the University of Massachusetts are the targets of multiple thefts and vandalism of high-value technical and computing equipment from both in and outside of the campus community. This report summarizes the recommendations of the Faculty Senate University Computer and Electronic Communications Committee (FSUCECC), in conjunction with Campus Police, to help stem this most recent wave of criminal activity.

## **Background**

In recent months, there were numerous attempts on campus to steal valuable audio-visual, computing and other high-value technical equipment from classrooms, laboratories and offices across campus. The Campus Police believe a number of these crimes are perpetrated by people outside the campus community, who come onto the University of Massachusetts with the hope of finding unsecured, high-value items that easily can be sold to fund other criminal activities. In response to these crimes, the Faculty Senate University Computer and Electronic Communications Committee (FSUCECC) met with Campus Police to determine what can be done from a faculty perspective to help stem these incidents, make our campus safer and prevent the loss and damage of university equipment.

## **Recommendations**

a. General Recommendations for all Faculty and Staff:

i) **SECURE CLASSROOM AUDIO-VISUAL EQUIPMENT.** Remember to lock up the Audio-Visual cabinets when you are done with the classroom. If possible, lock classrooms at the end of the day to further deter nighttime break-ins. Do not leave laptops and other easily removable equipment in classrooms when they are not in use, especially overnight.

ii) **LOCK YOUR OFFICES WHEN YOU LEAVE.** Campus Police, while conducting random walkthroughs of buildings, are finding multiple offices left open while faculty are teaching classes, attending meetings, going on breaks or leaving for the day. These offices have computers, purses, wallets, personal computing devices and other high-value items easily available for the taking. By taking away the opportunities, we can discourage off-campus people from using this university as an easy target for theft.

iii) **PASSWORD PROTECT YOUR SCREENSAVER AND SET IT TO ACTIVATE AFTER NO MORE THAN 5 MINUTES OF DOWNTIME.** This will prevent unwanted use of your equipment and unauthorized persons from accessing your email, SPIRE accounts and other private information.

iv) **DO NOT SAVE YOUR PASSWORDS WITHIN YOUR WEB BROWSER OR WRITE THEM DOWN WHERE OTHERS COULD ACCESS THEM.** This also will prevent unauthorized persons from accessing your private accounts.

b. Other (Non-Faculty) Recommendations to Improve Overall Campus Security:

i) ENSURE CAMPUS POLICE ARE NOTIFIED WHEN AUDIO-VISUAL EQUIPMENT ALARMS ARE SOUNDED. These notifications currently go to the office monitoring the audio-visual equipment for maintenance problems. These notifications also should be sent to Campus Police to ensure timely response both during the day and after normal working hours and on weekends.

ii) ENSURE ONLY AUTHORIZED CAMPUS PERSONNEL HAVE ACCESS TO ACADEMIC BUILDINGS, ESPECIALLY AFTER HOURS AND ON WEEKENDS. Many schools have implemented proximity cards and other measures that allow students and faculty access but prevent other personnel from entering. These systems can be programmed to provide extremely open access to some campus areas and restricted access to others. Access can also be restricted by time, date, etc. These measures will provide an additional layer of security to our academic facilities, again protecting university property and deterring persons from seeking out this university as a target.

**MOVED:**      **That the Faculty Senate approve the recommendations of the University  
29-07            Computer and Electronic Communications Committee to improve Security  
                    of Computing and Technical Equipment in Academic Spaces, as presented in  
                    Sen. Doc. No. 07-028.**