Minimum Security Standards for Networked Devices (DRAFT)

Faculty Advisory Committee Overview

October 2011 Meeting Information

Past Meeting Notes

Advisory Committee Charter

Advisory Committee Members

Introduction

Access to and use of the UCI electronic communications network (UCInet) is a privilege accorded at the discretion of the University of California, Irvine. Any device connected to UCInet must comply with minimum security standards as set forth in this policy. Devices that host restricted data as defined in University of California Business and Finance Bulletin IS-3 are required to conform to more rigorous security standards. Campus and Medical Center departments, units, or service providers may develop stricter standards as needed. Devices that do not meet the minimum standards for security may be disconnected from the network or have their network access restricted to minimize exposure to attacks.

UC Irvine staff, faculty, students and other affiliates are encouraged to use UCInet in the pursuit of education and research, and to conduct University Business. UCI's network resources are limited and vulnerable to attack and unauthorized use. UC Irvine therefore reserves the right to deny UCInet access to devices that do not meet the minimum standards for security. This policy is designed to not only protect individual devices, but other devices on UCInet that could be affected by a compromised or exploited device.

This policy applies to all devices connected to UCInet or using a uci.edu Internet Protocol (IP) address. It applies regardless of how the device is connected to UCInet and to any and all devices. Devices include computers, printers or other network appliances, network equipment, firewalls, Network Address Translation (NAT) devices, and mobile computing devices (laptops, PDAs, tablet computers, etc). Connection types covered include wired, wireless (mobile access), dial-in modem, and VPN services. Home systems using a VPN service, dial-in modems, or any other connection arrangement that give the connecting device a UCI IP address must meet this standard.

Responsibilities

Department Heads:

- Ensure that computers and devices connected to UCInet are supported by a system administrator or user with the ability to maintain minimum security standards.
- Support the efforts of School/Unit Computing Coordinators and other computing support staff in disseminating information about this policy and implementing it.

School/Unit Computing Coordinators (SCCs):

- Serve as the principal coordination point for compliance with this policy in each School or Unit.
- Ensure that all computers and network connected devices they or their staff manage comply with the minimum security standards listed in Appendix A.

System Administrators (or anyone functioning as one):

- Ensure all computers or network connected devices in their care comply with the minimum security standards listed in Appendix A.

Office of Information Technology (OIT):

- Work with the UCI community to protect computers and UCInet from attack, and block devices from UCInet or Internet when the security of the device is compromised.
- Support campus-wide information dissemination about, and implementation of, this policy.
- Facilitate access to security software required on each computer.
- Create/maintain tools for Computing Support Coordinator use in helping to manage devices connected to the network.

- Periodically review requirements enumerated in Appendix A with School/Unit Computing Coordinators, the OIT Faculty Advisory Committee, and others to ensure they continue to protect campus network security.

Minimum Standards

Minimum security standards for devices connected to UCInet are attached to this document as Appendix A: Minimum Standards for Security of Devices on UCInet. These standards can change periodically, so system administrators/end-users should consult the appendix to make sure they have the latest security standards before upgrading or changing devices connected to UCInet. Information and references providing guidance in implementing the minimum security standards are attached as Appendix B: Implementation References for the Minimum Standards for Security of Devices on UCInet.

Exceptions

Devices that are unable to comply with this policy must not be connected to UCInet unless an exception is granted to the school, department, or unit operating the device. Exceptions may be granted in circumstances where application of security patches may affect the operation of the device, application(s) running on the device, or operation of any attached instrument(s). In cases where exceptions are granted, the device given the exception will have its network access limited to the parts of UCInet necessary for its operation. Off-campus network access will not be allowed for devices granted exceptions.
To request an exception, please contact OIT@UCI.EDU with details on what the device is and why it needs an exception to this standard.

Updated: February 17, 2010