California State University Sacramento
College of Engineering and Computer Science

ECS IT Security Practices

January 12, 2017

College of Engineering and Computer Science (ECS) IT Security Practices are outlined below and in the ECS Information Security Plan. In addition, the College has an active Disaster Recovery Plan in place. The ECS IT Strategic Plan also discusses the College's commitment to balancing security needs with innovation and high functionality.

ECS Computing Services is the organization within the College of Engineering and Computer Science tasked with the responsibility to implement and monitor these practices. ECS Computing Services personnel keep up to date on security issues.

Physical security is well managed in the College. There are locks on all publicly accessible workstations. All network closets are locked and only key personnel have access to them. The main distribution point where the network backbone is located is behind two sets of locked doors, with different keys and monitored by internet security cameras.

The College utilizes off-site backup of critical information. Critical servers are mirrored daily and there are full weekly and monthly backups.

The College has a high-level intrusion detection and an intrusion prevention system, beyond the ECS firewalls and virus protection methods.

Faculty, staff and students are kept apprised of all security issues through technology update notices, timely bulletins, and meeting notifications.

The following security practices exist to protect the ECS network:

- All systems require secure user authentication. There is a single unified login for all ECS Windows, MacOS and UNIX systems authenticated by an NIS server.
- Student project and experimental systems requiring administrator privileges are isolated from the rest of the network through firewall policies.
- Incoming traffic is monitored, and if appropriate blocked, by the

ECS firewalls.

- All official ECS web pages reside on, or are an extension of, www.ecs.csus.edu. Official web pages are those that represent the College and are approved by the Dean, Department Chairs or other heads of specific units.
- All ECS web pages containing sensitive, confidential or restricted information are accessed via secure logins through the ECS Web Portal Page.
- All unofficial ECS web pages generally reside on, or are an extension of, gaia.ecs.csus.edu/~USERNAME. Unofficial web pages are those that represent specific students or faculty/staff and not the College. Unofficial pages conform to College and University appropriate use policies.
- IP addresses used on the ECS network must be assigned by either the ECS DHCP server or ECS Computing Services.
- Software that uses SNMP or ICMP to automatically "discover" or identify entities on a network generally can have a negative impact on the network at large. ECS Computing Services should be notified before such tools are run on the ECS network.
- Each ECS server has its own individual security systems and processes.
- ECS user accounts are generated with random passwords, and when changed by the user must conform to a prudent “hard-to-crack” convention.
- The latest virus protection software, software patches, Service Pack (SP) fixes, upgrades to supported/licensed products, etc. are distributed through the ECS Windows Update Server and various UNIX-based update distribution systems.