Physical Security of EMCC Computer and Network Resources

Network Access

In order to protect computing resources from malicious and unauthorized access, every VLAN is protected with a virtual firewall context. In addition, every computer on campus, both client and server, have host based firewalls configured. This provides a second layer of security in case the network firewall is breached. Firewall rules are configured so that only specific traffic is allowed and all other traffic is denied.

Physical Access

Physical access to sensitive college computing areas, such as telecommunications closets and the server room are restricted to only authorized employees. This includes Network Services employees, the Director of Information Technology, Director of Facilities, college safety officers, and the HVAC technician. The server room and several telecommunication closets are protected with Proxima card readers and secured through the BASIS system. The balance of the telecommunications closets are secured with physical keys and will be retrofitted with card readers as funding permits. College Safety provides strict access control of keys to these resources. Cameras are trained on the main server room, video is recorded, and monitored by College Safety. In addition, a physical check is done every hour by College Safety during periods of campus closure.