University Senate Meeting, 04/11/2017
General Consent Item: Decommissioning HSU's Secure Space Physical Access Policy

The existing HSU policy on secure spaces, with limits on physical access for ITS equipment, is proposed for decommissioning. The relevant policy is at the CSU level; the campus is assigned responsibility for designating the relevant rooms and other spaces where this equipment is maintained. As such, it doesn't rise to the level of policy. Moreover, in its current form, the spaces designated are not up to date. With the decommissioning of this policy, it will be clearer that the CSU policy is operative and ITS will maintain the relevant list of spaces and procedures used at HSU to implement this policy.

A copy of HSU's policy which is being recommended for decommissioning is attached.

Published on *HSU Policies* (http://www2.humboldt.edu/policy)

EM:P11-11 HSU Data Center and Telecommunications Physical Access Policy

Month/Year Posted: 2011-11
Policy Number: EM:P11-11
HSU Data Center and Telecommunications Physical Access Policy

Background

The California State University Information Security Policy is published at http://www.calstate.edu/icsuam/sections/8000/ [1]. Section 8080 titled "Physical Security" requires that physical areas such as Data Centers must be protected from unauthorized physical access while ensuring that authorized users have appropriate access.

The following Humboldt State University facilities are high security technical areas:

Data Center: VMH211, SH005A

The HSU Data Center (VMH211) is a consolidated server room designed to provide 24/7 operations with redundant environmental, power, physical and network controls for HSU servers which deliver enterprise-wide, mission critical applications, and to protect electronic stores of institutional data which are subject to privacy regulation by CSU, state and federal policies/laws (FERPA, HIPAA, PCI, Graham-Leach-Bliley, et al.).

The Secondary Data Center located in SH005 is equipped with security and environmental controls appropriate for its function as the first backup site for mission critical services.

Core Distribution Rooms: VMH211A, SH005B, NR001B

Core distribution rooms are located in Van Matre Hall, Siemens Hall and the Natural Resources Building. Core distribution rooms may contain campus information technology infrastructure systems, firewalls, campus backbone core switching routers, and telephony equipment including 911 emergency and voice switch systems.

Telecommunications Rooms:

Telecommunications rooms are delimited and are protected areas where data and phone

cables within a building or a portion of a building are connected to campus networking equipment. Telecommunications rooms exist in all buildings on campus.

Policy

All requests for access to the HSU Data Center and telecommunications areas must be approved by the Chief Information Officer (CIO) or designee. Access will be restricted to specific individuals with job functions related to operating mission critical equipment in the Data Center, core distribution rooms and telecommunications rooms. Job functions eligible for approval are:

- ITS System Administrators
- ITS Network Analysts
- Public Safety personnel
- Plant Operations Electricians
- Plant Operations Heating and Ventilation Engineers

The CIO or designee must approve all changes to physical controls such as locks and alarm codes.

The Information Security Officer (ISO) will maintain procedures related to physical security and access to the Data Center, core distribution rooms and telecommunications rooms. Compliance with the following Data Center procedures is required:

- HSU Data Center Physical Access Procedure
- HSU Network Spaces Physical Access Procedure
- Data Center Physical Access Training Procedure

Prior to being granted any unrestricted or unescorted physical access, individuals must:

- Have a signed confidentiality agreement on file
- Complete a "Live Scan" background check
- Complete Data Center Access Training as defined by the Information Security Officer (ISO)

Compliance

Unauthorized access to locations defined in this policy must be reported to University Police and the Information Security Office.

Violators of this policy are subject to disciplinary action up to and including dismissal from employment, expulsion from the University, and civil or criminal prosecution, as appropriate. Disciplinary action shall be conducted in accordance with applicable collective bargaining agreements or other appropriate University policies.

Source URL (retrieved on *2017-03-29 20:18*): http://www2.humboldt.edu/policy/PEMP11-11HSU-Data-Center-and-Telecommunications-Physical-Access-Policy

Links:
[1] http://www.calstate.edu/icsuam/sections/8000/