California Health Sciences University

CHSU NETWORK SECURITY AND SECURITY OF DEVICES CONNECTING TO THE NETWORK

I. PURPOSE

The purpose of this policy is to provide direction for managing network security, including log event management, protecting network connected devices, including mobile devices from malicious software, and vulnerability management.

II. INFORMATION TECHNOLOGY SECURITY

CHSU will develop and implement appropriate technical controls to minimize risks to the university technology infrastructure. Each college and department must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protect data from threats.

III. PROTECTIONS AGAINST MALICIOUS SOFTWARE PROGRAMS

A. CHSU must have plans in place to detect, prevent, and report malicious software effectively. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a non- quarantined location on a campus network or information system.

B. All computing devices that connect to the University network infrastructure, including all off-campus devices connecting remotely (e.g., via the virtual private network -VPN) must be protected with anti-virus software or by other appropriate means. All anti-virus software shall conform to campus standards and shall have up- to- date virus definitions. This applies to all computing devices, regardless of ownership or location.

IV. NETWORK SECURITY

CHSU will design its networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity, and availability of university data and systems. CHSU will regularly review how protected data is transmitted-over the campus network. This process includes the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus systems. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

V. INFORMATION ASSET MONITORING

A. CHSU will implement appropriate controls on the monitoring of information systems and network resources to ensure that monitoring is limited to approved activities. Monitoring must not be conducted for the purpose of gaining unauthorized access, “snooping,”, or for other activities that violate the CHSU Acceptable Use of Technology Policies.

B. Records created by monitoring controls (e.g. logging) must be protected from unauthorized access and reviewed regularly. CHSU will ensure that only individuals who have a “need-to-know” are granted access to data generated from monitoring controls.

C. Data generated by monitoring will be retained for a period of time that is consistent with effective use, CHSU records retention schedules, regulatory, and legal requirements such as compliance with litigation holds. At a minimum, system administrators will scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed.

VI. RISK FACTORS THAT WILL BE CONSIDERED:

A. Criticality of business process.

B. Information classification associated with the system.

C. Past experience or understanding of system vulnerabilities.

D. System exposure (e.g., services offered to the Internet).

- Policy Owner: Executive Director of Information Technology
- Effective Date: 9/02/2020
- Revised Date:
- Approval by the President: 09/14/2020