Division:
Administration & Finance

Department:
Information Technology Services

Contact Information:
Nish Malik / Associate Vice President and Chief Information Officer, Information Technology Services / (415) 405-4105 / nish@sfsu.edu

Effective Date:
Monday, September 14, 2020

Authority:
ICSUAM 8000 - Information Security Policy
ICSUAM 8045 - Information Technology Security
ICSUAM 8105 - Responsible Use Policy
ICSUAM 8050.s200 – High Risk and Critical Workstation Standard

Objective:
The Network Practice Directive defines the campus requirements to protect SF State University’s network infrastructure from unauthorized use, eavesdropping, and targeted attacks that could result in loss of information, damage critical applications, or impact University operations.

Statement:

Purpose & Scope
All users (faculty, staff, students and community members) using the university network must follow University-defined practice directives, processes and use University-managed network devices and wireless access points. All changes to campus network services are made by Information Technology Services (ITS).

- SF State network users must comply with the CSU Responsible Use Policy
- Devices on the SF State network must comply with endpoint/mobile device standards
- The SF State network may require users to have a current affiliation and authenticate
- The SF State network may require the installation of network access control software
- Authenticated secure remote access is available to faculty and staff. Other users may be provisioned with an approved business justification.
- All wired and wireless, remote access, and network security services are centrally managed by ITS
- Network equipment that is not centrally managed by ITS will be disabled to be compliant with CSU Common Network Initiative (CNI) standards
• The SF State network must provide protection controls to address the requirements identified in the High Risk and Critical Workstations standard. Requirements include the following:

a) Network traffic is limited to the minimum necessary to perform business functions by use of isolated network segment with traffic restricted to authorized inbound and outbound ports and destinations. This requirement may be satisfied in combination with a virtual desktop environment for other work functions (web browsing, etc.) in order to address productivity.

b) Intrusion detection and prevention technologies which address hostile sites, malware, etc.

c) Software defined networking, user based and/or application-defined routing or similar use of technology to control connectivity.

Implementation

Responsibility for implementing this Practice Directive will rest with ITS and departments across campus. Submit any apparent violation of Network Practice Directive to the appropriate administrative authority (vice president, dean, director, department, or program chair) or to service@sfsu.edu.

Non-Compliance

Noncompliance with applicable policies and/or practices may result in suspension of network access privileges. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.