The UC Berkeley Minimum Standards for Security of Berkeley Campus Networked Devices

1. Keep software patches current
2. Run approved anti-virus software
3. Run approved host-based firewall software
4. Use secure passwords
5. No unencrypted authentication
6. No unauthenticated email relays
7. No unauthenticated proxy services
8. Ensure physical security
9. Don’t run unnecessary services

Minimum Standards for Security of Berkeley Campus Networked Devices
The following minimum standards are required for devices connected to the campus network.

1. Software patch updates
   - Campus networked devices must run software for which security patches are made available in a timely fashion. They also must have all currently available security patches installed. Exceptions may be made for patches that compromise the usability or critical applications.
2. Anti-virus software
   - Anti-virus software for any particular type of device currently listed on the Campus software distribution website (https://software-berekeley.edu) must be running and up-to-date on every device, including clients, file servers, email servers, and other types of campus networked devices.
3. Host-based firewall software
   - Host-based firewall software for any particular type of device currently listed on the Campus software distribution website (https://software-berekeley.edu) must be running and configured according to the "Implementing guidelines for the campus standards for security of Berkeley campus networked devices," on every level of device, including clients, file servers, email servers, and other types of campus networked devices. When data protection software is being used, the software must be configured to block any unnecessary services.
4. Passwords
   - Campus electronic communication systems or services must identify users and authorize access by means of passwords or other effective means of access control (e.g., biometrics on security cards). When passwords are used, they must meet the "Minimum password management standards." In addition, shared access patterns must enforce these standards; otherwise, passwords must not be used, change, or implement patterns to ease access to the network.
   - All default passwords for access to network-accessible devices must be changed. Passwords used by system administrators for their personal access to a service or device must not be the same as or similar to passwords for privileged access to any service or device.
5. No unencrypted authentication
   - Unencrypted device authentication mechanisms are only acceptable on the network where they are used. Traffic on the campus network must be encrypted to maintain the integrity of data exchanged, including all security authentication mechanisms and services. Therefore, campus devices that use any unencrypted authentication mechanisms must be authenticated by the CSIC (See "Precautions for Encryption" in the Berkeley Campus Policy on Network Standards for Network Device Security).
   - In particular, network access services such as Telnet, FTP, SMTP, POP, and LDAP must be replaced by their encrypted equivalents.
6. No unauthenticated email relays
   - Campus devices must not provide an active SMTP service that allows unauthenticated third parties to relay email messages, i.e., to process email messages where neither the sender nor the recipient is a valid user. Before transmitting email to external hosts, the sender must authenticate with the SMTP service. Authenticating the machine (IP of outside domain) rather than the sender is not sufficient to meet this standard. Unauthenticated email relays have been identified by the CSIC and have been removed by the CSIC as an action against and appropriate use. It may not operate on the campus network.
7. No unauthenticated proxy services
   - Although properly configured unauthenticated proxy services may be used for specific purposes, each service must be certified by a means of appropriate device configuration. Unauthenticated proxy services may only be enabled on the network if the device is being used in the context of an authorized user. Therefore, unless unauthenticated proxy services are included in the standards developed, the standards developed by the CSIC to configure and appropriate use, or not on the campus network.
   - In particular, unsecured proxy service, unsecured email servers, and unsecured email servers are automatically enabled in the "guidelines for the campus standards for security of Berkeley campus networked devices, 8. Physical security
   - Unauthorized physical access to an unauthorized device can result in harmful or fraudulent misappropriation of data, fraud, misappropriation of data, and/or any other physical property. In light of this, it is on the campus network.
   - If a service is not necessary for the intended purpose or operation of the device, the service and not running.

Policy Foundations for Secure Computing

Everyone is Responsible for Securing Electronic Resources
- Each campus community member is responsible for securing and protecting electronic information resources he or she controls.
- Academic employees are also administrators of electronic information resources.
- Protected resources include networks, computers, software, and data.
- Resources must be protected against unauthorized intrusions, malicious misuse, or inadvertent compromise.
- Activities outsourced to off-campus entities must comply with the same security requirements.

Active Data Stewardship is Required
LAW: SB1386 implementing procedures prompting development of minimum standards (see Berkeley Campus Plan Implementing the UC Requirements for Protection of Computerized Personal Information)
http://policy.berkeley.edu/protectdata.html

POLICY: Data Management Use Policy (DMUP)
- Articulates information management policy.
- Standardizes terms and procedures for data use.
- Defines data stewardship roles, responsibilities, and best practices.
- Establishes a system for resolving disputes about who controls administrative data.

Electronic Resources Security is Centrally Coordinated
- To be connected to the network you must have the expertise to properly set up your computer or get help from someone who does have the expertise.
- Central campus experts monitor all network traffic.
- You can be disconnected or blocked from the network if your computer is compromised.
- Guidelines clearly detail circumstances under which connections can be blocked by UCB System and Network Security.
- Every campus department and unit has a security contact.