



Vulnerability Management Standard [ISEC 12.6]

OWNER Jason Musselman
APPROVED BY Brooke Banks, ISO
ISSUED 7/8/2008
CALIFORNIA STATE UNIVERSITY, CHICO

REVIEW 11/5/2008
Page 1 of 1

Purpose

The campus Vulnerability Management Standard provide system owners, server administrators and application administrators with a standard set of effective, systematic, repeatable and measurable processes that map to ISO 27002 (17799), Section 12.6.

Background

CSU, Chico procured a vulnerability management suite (VMS) from McAfee called Foundstone. Foundstone is used by server administrators to identify, remediate and provide reports to system owners and application administrators of system vulnerabilities. The Information Security Office maintains a server registry and uses the registry data to populate Foundstone with system information and user accounts for server administrators.

Standard

Server Administrators, as defined in the *System Roles and Responsibilities* (ISEC 6.1) document, are required to regularly scan, remediate and report un-remediated vulnerabilities to the system owner or application administrator within a prescribed timeframe.

The following list of tasks is required to protect campus system and network resources.

1. Server Administrators perform specified weekly, monthly and quarterly scans and tests as described in the *Vulnerability Scanning Procedures & Guidelines* (ISEC 12.6).
2. Server Administrators remediate or provide remediation plans to system owners within 24 hours for any high-risk vulnerability and within 5 days for vulnerabilities rated as important.
3. Application Administrators remediate and or provide remediation plans to system owners and server administrators within 24 hours of notification on any high-risk vulnerability and within 5 days for vulnerabilities rated as important.
4. The System Owner accepts the risk of any un-remediated vulnerability for systems under their control.
5. The System Owner report and maintain a log of un-remediated vulnerabilities detailing the mitigating factors and level of risk to the system for review by the Information Security Office.
6. Server Administrators must allow the vulnerability scan engine to scan all services provided on their systems. For systems with defined access control lists or policies, access must be granted to allow the vulnerability scan engine to scan the service for vulnerabilities.