ISSUE DATE: March 13, 1997 REVISION DATE: February 15, 2000	POLICY: Operating System Software Maintenance
REFERENCE:	
APPROVED: /s/ Jerry A. Aspland	

I.   Policy Statement

System *owners* and system support personnel use *system software* to allocate, manage, and to control access to system resources. System software must be controlled and maintained properly by authorized personnel to ensure that application systems continue to operate properly.

II.   Principles

System software maintenance standards, procedures, and conventions must be established to help ensure the integrity of data and operating effectiveness. They also help control access to system resources. System software will be maintained in compliance with Policy 208.4, *System Administration*.

The Information Systems Department is responsible for the development of operating system software standards.

III.   Deployment

All new system software must be tested and approved by the Information Systems (IS) Department. Authorized personnel must install all system software. Formal change control procedures must be used to ensure that only authorized changes are made to system software.

IV.   Technical Architecture

System software maintenance procedures include the use of standard naming conventions and program documentation requirements.

Controls are needed to ensure that:

1. Only authorized system software and changes are placed into production.
2. Only authorized personnel move system software changes from the test environment into the production environment.
3. Maintenance procedures also include the tracking of system software installation, change requests, approvals and *back-out procedures*.
4. All system software used by critical applications must not be more than two releases behind the current release.

All system software must be backed up periodically according to the requirements in the Disaster Recovery Plan.

V.   Monitoring

The IS Department and resource owners are responsible for identifying system software upgrades and if they are necessary to meet campus goals and objectives. Periodic reviews of system software will be conducted by the IS Department to ensure that only authorized changes have been made.

System software problems should be reported, logged and resolved in a timely manner.

Technical support agreements must be reviewed and re-evaluated periodically (at the end of the initial term or renewal term, whichever is the earliest) to ensure the agreements still accurately reflect Cal Maritime's computing requirements.

VI.   Documentation Requirements

All system software must have complete and updated documentation. A complete inventory of all system software must be kept current by the IS Department. All system software installation, change requests, test results, approvals, and program moves into production will be documented and retained by the IS.

The IS Department will also keep technical support agreements for system software on file.

VII.   Definitions

System software: Operating and sub systems. This includes software such as communication server software, network operating systems software, and operating systems software (e.g. Windows NT server software).

Owner: A designated person who is responsible for system and user administration functions including system maintenance and add/change/delete access granted.

Back-out procedures: Allow the timely and expedient recovery to the prior version of the operating system software in the event of a failed installation or change.

VIII.   References

System Administration, Policy 208.4