SYSTEM LIFECYCLE MANAGEMENT 0951

(No.16 September 2004)

PURPOSE

This policy establishes the life cycle requirements of CAL FIRE's automated information technology systems, approvals, and roles and responsibilities for implementing this policy. Observance of this policy will ensure full value is obtained from investments in data and information systems.

SCOPE AND APPLICABILITY

All automated information technology systems that are developed, produced or maintained by or for the CAL FIRE are subject to this policy. This policy applies to all CAL FIRE organizational units and their employees. It also applies to agents or contractors of the CAL FIRE who support the initiation, analysis, design, development, operation and retirement of CAL FIRE information systems.

BACKGROUND

The CAL FIRE depends on information to accomplish its mission. CAL FIRE's data and information systems are valuable information assets and are critical to the CAL FIRE's ability to accomplish its mission. Development of information systems is difficult, and often complex and expensive. The system life cycle management policy is designed to meet applicable product and program requirements, ensure management involvement at key decision points, obtain and sustain commitment for information systems, and coordinate information systems-related activities.

System life cycle management promotes involvement by users, program managers and information resource managers in system development and enhancement efforts. It establishes a process by which CAL FIRE managers are directly accountable for making key decisions about how resources are expended for system development and enhancement efforts.

CAL FIRE relies frequently upon contractors and other partners for assistance in building and operating its information systems. System life cycle management establishes practices and periodic review requirements that mitigate the uncertainties involved in using extramural support.

POLICY

a. All information systems shall support the mission of the CAL FIRE. System Management Plans for information systems shall be generated and included in CAL FIRE and organizational budget and planning processes as appropriate.

b. All CAL FIRE locations and active projects will submit a Systems Management Plan yearly; due on November 1st. This plan will encompass all systems deployed within the unit or project.

c. Units (or projects) that do not submit a Systems Management Plan will not be allowed to purchase Information Technology Equipment.

d. All units will maintain technology infrastructure as articulated in the asset management plan, Computer Hardware Allocations and Standard Complement section. Unit's that desire to increase or decrease the compliment must seek approvals from their Region Chief, Deputy Director and the CIO as needed.

e. CAL FIRE Technology Assets will not be supported, and will be pulled from the CAL FIRE computing environment if they have exceeded their planned lifespan unless an exemption is approved by EMC.

f. All information systems shall comply with appropriate State, Agency, and CAL FIRE policies, standards, security policy, and procedures throughout their life cycles.

g. Systems and equipment already deployed that do not meet planned lifecycle criteria require the initiation of system upgrade projects to ensure conformance.

h. CAL FIRE personnel will ensure Information Technology Assets are maintained to the following lifespan schedule:

Asset	Planned Lifespan Schedule
Personal Workstation	4 Years
Printer	4 Years
NT File and Print Servers	4 years
Database Servers	5 years
Wide Area Network	7 years
LAN Cable Plant / Network devices	7 Years
Remote Access Services (RAS)	5 Years
Terminal Server	4 Years
Core Network Devices	5 Years

EXEMPTION PROCESS

Unit's and Programs that cannot maintain Information Systems to the lifecycle schedule in this policy due to funding limitations may submit an explanation as part of the system management plan.

SYSTEM MANAGEMENT PLAN

The System Management Plan (SMP) shall be produced yearly. For projects, the Systems Management Plan will be submitted at the conclusion of the analysis stage, and shall be updated yearly as the project progresses. The following Table sets forth required CAL FIRE management review levels for System Management Plans.

CAL FIRE system management plan / review level threshold criteria

SYSTEM CATEGORY	THRESHOLD CRITERIA (System category is determined by the highest threshold reached under either the scope OR cost criteria OR telecommunications criteria			SYSTEM MANAGEMENT PLAN(SMP)MUST BE APPROVED BY:
	Scope	Cost	Telecommunications	
1 - Major Mission Critical System	Critical for multiple Units, Regions	>$5 million throughout the lifecycle or $1 million annually	Extensive use of WAN or Internet communications	Project Manager, Relevant Deputy Director, CIO, and Director
2 - Major Unit or Regional System	Critical for multiple Units or Regional Implementation	>$1 million throughout the lifecycle or >$100,000 annually	Uses WAN or Internet Communications	Project Manager or AO, Relevant Deputy Director, and CIO
3 - Significant Program System	Critical in Single Program Office	>$100,000 throughout the lifecycle or >$50,000 annually	Uses WAN or Internet Communications	Project Manager or AO, and CIO
4 - Local office or Individual Use System / Work Group Computing	Systems Below Category 3 Thresholds or replacement PC / Printer project	<$25,000 annually for one project	No WAN or Internet Communications needed	Project Manager or AO

Note: Some applications and projects utilize socialized resources, including but not limited to database or application servers. Socialized resources are the funding responsibility of EMC, and will be submitted as part of the enterprise resources system management plan.

RESPONSIBILITIES

i. The Executive Management Committee (EMC) is responsible to:

- Review and approve/disapprove policy
- Review and approve/disapprove funding for System Management Plans for major mission critical systems and enterprise assets

j. The Information Technology Advisory Committee (ITAC) is responsible to:

Ensure procedures and processes associated with the asset management plan are functioning, and up to date

k. The Chief Information Officer (CIO) is responsible to:

- Enforce the Systems Management Plan policy and procedure.
- Review and approve/disapprove System Management Plans for Major Mission Critical Systems, Major Unit or Regional Systems, and Significant Program Systems.
- Review and approve/disapprove risk assessments for EAC/EMC consideration related to asset management
- Conduct, at his/her discretion, additional system life cycle management reviews to complement the reviews required to be conducted periodically by system sponsors and Administrative Officers
- Provide technical consultation to reviewers of System Management Plans concerning the description of the system's architectural context, technical requirements, anticipated security issues, platform and network capacity needs to ensure conformance with the CAL FIRE's Enterprise Architecture.
- Prepare Annual report of status of lifecycle to EMC
- Ensure procurement and support policies are adhered to.
- Maintain Supported and Non Supported hardware and software lists

l. Administrative Officers and Product Sponsors are responsible to:

- Submit a Systems Management plan yearly, due on October 1st. This plan (SMP) will encompass all of the technology (PC’s, Printers, Applications etc.) hosted in the area of responsibility for the administrative Officer or Sponsor.
- Ensure compliance with system life cycle management policies, procedures and standards.
- Manage the system life cycle, process and products within their organizations in compliance with CAL FIRE policy.
- Conduct periodic system life cycle management reviews to evaluate costs and efficiency of operation, and ensure the system is continuing to meet mission needs.

m. Each CAL FIRE employee engaged in system life cycle management activities is responsible to:
Conform to this policy, and related procedures and standards.

(*to be written*) 0951.1

OPERATING SYSTEM SUPPORT POLICY 0951.2

(No.19 August 2005)

PURPOSE OF POLICY

This policy ensures the CAL FIRE networks and computers are not compromised by lack of security or stability by obsolete hardware and obsolete software.

BACKGROUND

Information Technology Services does not currently have an approved hardware or software support policy. It is the intent of the department to create and maintain a robust and comprehensive Information Technology support policy, but this may take significant time to develop and approve. In the interim, ITS is required to manage various elements of the CAL FIRE enterprise to ensure security and supportability. Recent Microsoft security issues have exposed the CAL FIRE to significant risk from obsolete Microsoft Operating systems, as Microsoft is no longer supporting automated methods for security updates on older products to ensure their products are protected. Costs associated with manually updating these computers can run up to $50,000 per security event.

POLICY

Information Technology Services has standardized support for Microsoft Operating Systems in line with the manufacturer. Microsoft supports operating systems 6 years from release, with an additional 2 years specialist paid support to EOL (end of life) of its software. This includes bug fixes, security updates and technical support.

- ITS does not support Microsoft Operating systems deemed obsolete by Microsoft.
- Currently, ITS only supports Windows 2000 and Windows XP professional operating systems on personal computers.
- Computers running obsolete operating systems will be permanently disconnected from the CAL FIRE network as of February 1, 2006.
- Computers running obsolete operating systems must be removed completely from the CAL FIRE deployed inventory by February 1, 2006.

(see next section)

(see HB Table of Contents)

(see Forms or Forms Samples)