

ANNUAL EVALUATION OF EFFECTIVENESS OF INFORMATION TECHNOLOGY MANAGEMENT PLAN

FY 2026-2027

Overall Evaluation of Effectiveness Statement

The Information Technology (IT) division's safety program is designed to ensure that critical safety systems managed by IT are regularly checked, monitored and tested throughout the year. Scheduled, periodic maintenance (PM) is performed on these systems consistently due to their importance to patient safety. IT takes these PM activities seriously and they regularly achieve 100% during PM checks (minimum allowable is 95%).

Evaluation of Scope & Responsibilities

The scope of the department Utility Management plan is to identify the scope of work to be performed in response to Utility Management, Information and Communication Systems, and to assess the performance and effectiveness of the plan.

IT departments promote a safe, controlled, comfortable environment of care by defining the critical systems we support. We identify the scope of work to be performed in response to Utility Management and assess the performance and effectiveness of the plan by implementing policies and procedures to ensure reliability of these systems, minimize the risks associated with a system failure and evaluate the failures to put processes in place to reduce the risk of a re-occurrence.

Adherence to the policies and procedures is handled through monitoring and of performance indicators, which are identified in our Preventive Maintenance program. Information Technology committees are meeting to determine the need and/or requirements for future Information Technology critical systems.

In addition, we are continually initiating recommendations and/or evaluating options to improve the effectiveness of the ten critical utility systems that IT Departments are responsible for;

Nurse Call	800MHz Radio Systems
Fire Alarm Systems	Code Blue System
Overhead Paging System	Abduction Alarm System
Elopement Alarm System	Call Manager (VoIP Phones)
Backup Private Branch Exchange (PBX)	Main Telephone Private Branch Exchange

The assessment and minimization of risks to critical utility systems supported by IT departments are a pro-active process that includes the proper design as defined in specifications utilized when systems are installed, and accurate implementation of systems being installed through ongoing project management. The development of recovery plans, which identify all back-up systems to be utilized for each critical system supported by the IT departments, provides us with the ability to recover from a system failure in a systematic way. Scheduled maintenance is monitored by performance assessment based on identified indicators and initiating continuous improvement by evaluating options for enhancements to the design and/or redundancy required to support the critical systems supported by IT departments.

Emergency procedures for critical systems

Information Technology Departments have in place an Emergency Management plan, which identifies the critical systems supported, and the following actions:

Critical System Back-Up Components
Primary, Secondary, Vendor Contacts
Recovery Set-up Time

Ensuring Operational Reliability
Impact and Response Back-up Systems
Other Options

To ensure operational reliability of the critical systems supported by the IT Division in a combined effort with Plant Operations and Maintenance, Fire Services, and outside vendor support managed by Information Technology. Preventive Maintenance schedules are coordinated, back up critical system support is identified, and/or when applicable network optimization to reduce the amount of downtime for the critical systems that are linked via the Wide Area Network are monitored and managed by Information Technology.

Identification, Evaluation, and Inventory of Critical Systems

The establishing of criteria for identifying, evaluating, and taking inventory of the critical equipment supported by Information Technology is based on life support systems and voice communication systems. The establishment of criteria and the critical equipment inventory list are included in the Critical Equipment Maintenance policies and procedures. The policies and procedures identify a list of systems which are currently installed, and the procedures to follow to test the performance of said equipment. This information is updated in conjunction with the purchase of newer technology and/or critical systems.

Evaluation of Objectives

Objective 1: Minimize Risk of Utility Failure

Status: Objective met

The assessment and minimization of risks to critical utility systems supported by IT departments are a pro-active process that includes the proper design as defined in specifications. Recovery plans provides us with the ability to recover from a system failure in a systematic way. Scheduled maintenance is monitored by performance assessment based on identified indicators. Continuous improvement occurs by evaluating options for enhancements to the systems in order to improve overall reliability of systems supported by IT departments.

Objective 2: Emergency procedures for critical systems

Status: Objective met

Information Technology Departments have in place an Emergency Management plan, which identifies the critical systems supported, and the following actions:

Critical System Back-Up Components
Primary, Secondary, Vendor Contacts
Recovery Set-up Time

Ensuring Operational Reliability
Impact and Response Back-up Systems
Other Options

Objective 3: Ensuring Operational Reliability

Status: Objective met

To ensure operational reliability of the critical systems supported by the IT Division in a combined effort with Plant Operations and Maintenance, Fire Services, and outside vendor support managed by Information Technology. Preventive Maintenance schedules are coordinated, back up critical system support is identified, and/or when applicable network optimization to reduce the amount of downtime for the critical systems that are linked via the Wide Area Network are monitored and managed by Information Technology.

Objective 4: Identification, Evaluation, and Inventory of Critical Systems

Status: Objective met

The establishing of criteria for identifying, evaluating, and taking inventory of the critical equipment supported by Information Technology is based on life support systems and voice communication systems. The establishment of criteria and the critical equipment inventory list is included in the Critical Equipment Maintenance policies and procedures. The policies and procedures identify a list of equipment (inventory), which is currently installed, and the procedures to follow to test the performance of said equipment. This information is updated in conjunction with the purchase of newer technology and/or critical system.

Evaluation of Performance:
Key Program/Performance Measures
2025/2026

Systems - Preventative Maintenance Measurements	Goal	Achieved	Measured in 2025/2026?
Nurse call system scheduled maintenance	95%	100%	Yes
800 MHZ radio system scheduled maintenance	95%	100%	Yes
fire alarm system scheduled maintenance	95%	100%	Yes
Code Blue system scheduled maintenance	95%	100%	Yes
overhead paging system scheduled maintenance	95%	100%	Yes
Elopement & Abduction Alarms scheduled maintenance	95%	100%	Yes
Call Manager (VOIP phones) scheduled maintenance	95%	100%	Yes
back-up private branch exchange (PBX) scheduled maintenance	95%	100%	Yes
main telephone private branch exchange scheduled maintenance	95%	100%	Yes

Updated: August 03, 2026

INFORMATION TECHNOLOGY MANAGEMENT PLAN

Fiscal Year 2026/2027
UPDATED: September 01, 2026

INTRODUCTION & MISSION STATEMENT

The Utility Systems Management Plan is based on the Mission, Vision, and Values of University of California, Davis Health System. Additionally, the Management Plan incorporates the Local, State, Federal and Professional codes, standards, and regulations as applicable. Specifically included are city of Sacramento, County of Sacramento, State of California, OSHA, EPA, and Joint Commission codes, standards, and regulations.

The Utility Systems Management Plan is applicable to all University of California, Davis Health System entities. Whenever there is a Department/Service or site-specific variation, it will be supported by a Department/Service or site specific policy and procedure that are reviewed for overall Governing Body - Supports the management plan through Joint Management Council and through review and approval of Safety Committee quarterly and annual reports. Safety Committee reports are recommended for Joint Management Council attention by Medical Staff Executive Committee.

PLAN SCOPE & RESPONSIBILITIES

The scope of the department Utility Management plan is to identify the scope or work to be performed in response to Utility Management, Information and Communication Systems, and to assess the performance and effectiveness of the plan.

IT departments promote a safe, controlled, comfortable environment of care by defining the critical systems we support. We identify the scope of work to be performed in response to Utility Management and assess the performance and effectiveness of the plan by implementing policies and procedures to ensure reliability of these systems, minimize the risks associated with a system failure and evaluate the failures to put processes in place to reduce the risk of a reoccurrence. Adherence to the policies and procedures is handled through monitoring and of performance indicators, which are identified in our Preventive Maintenance program. Information Technology committees are meeting to determine the need and/or requirements for future Information Technology critical systems.

PRINCIPLES

- Information Technology systems play a significant role in supporting complex medical care and in providing an appropriate technological environment for providing safe patient care.
- Orientation, education, and training of Information Technology staff on building and maintaining resilient systems is an essential part of assuring safe effective care and treatment are rendered to people receiving services.
- Assessment of needs for continuing technical support of information technology systems and design of appropriate planned maintenance, and resiliency/recovery services is an essential part of assuring that the information technology systems are reliable.

LIST OF OBJECTIVES 26/27

Objective 1: Minimize Risk of Utility Failure

The assessment and minimization of risks to critical utility systems supported by IT departments are a pro-active process that includes the proper design as defined in specifications. Recovery plans provide us with the ability to recover from a system failure in a systematic way. Scheduled maintenance is monitored by performance assessment based on identified indicators. Continuous improvement occurs by evaluating options for enhancements to the systems to improve overall reliability of systems supported by IT departments.

Objective 2: Emergency procedures for critical systems

Information Technology Departments have in place an Emergency Management plan, which identifies the critical systems supported, and the following actions;

Objective 3: Ensuring Operational Reliability

To ensure operational reliability of the critical systems supported by the IT Division in a combined effort with Plant Operations and Maintenance, Fire Services, and outside vendor support managed by Information Technology. Preventive Maintenance schedules are coordinated, back up critical system support is identified, and/or when applicable network optimization to reduce the amount of downtime for the critical systems that are linked via the Wide Area Network are monitored and managed by Information Technology.

Objective 4: Identification, Evaluation, and Inventory of Critical Systems

The establishing of criteria for identifying, evaluating, and taking inventory of the critical equipment supported by Information Technology is based on life support systems and voice communication systems. The establishment of criteria and the critical equipment inventory list are included in the Critical Equipment Maintenance policies and procedures. The policies and procedures identify a list of equipment (inventory), which is currently installed, and the procedures to follow to test the performance of said equipment. This information is updated in conjunction with the purchase of newer technology and/or critical systems.

KEY PROGRAM/PERFORMANCE MEASURES

FY 2025/2026 EOC Key Performance Indicator, reported quarterly

Systems - Preventative Maintenance Measurements	Goal
Nurse call system scheduled maintenance	95%
800 MHZ radio system scheduled maintenance	95%
fire alarm system scheduled maintenance	95%
Code Blue system scheduled maintenance	95%
overhead paging system scheduled maintenance	95%
Elopement & Abduction Alarms scheduled maintenance	95%
Call Manager (VOIP phones) scheduled maintenance	95%
back-up private branch exchange (PBX) scheduled maintenance	95%
main telephone private branch exchange scheduled maintenance	95%

INFORMATION TECHNOLOGY MANAGEMENT ACTIVITY DETAIL

IT assesses and evaluates the ongoing performance regarding actual or potential risk related to staff knowledge and skills, by conducting staff annual training on each critical system supported as part of the Preventive Maintenance function. The target for completing preventative maintenance on critical equipment/systems is 95% each period (monthly/quarterly/semi-annually/annually depending on the system). If there are areas of deficiency in meeting the target these are noted in this report and the action taken to correct the deficiency is also documented.

There were no deficiencies noted for any of the critical systems PM evolutions during FY25/26.

Employees are required to perform the preventive maintenance assignments for each system supported throughout the year, which requires that they inspect, perform maintenance and test critical systems. As critical systems are installed or upgraded, the vendor trains the employees, and then the system is identified for annual training support. On a monthly, quarterly, semi-annual or annual basis, Preventive maintenance schedules are initiated and completed by technical staff. Monitoring adherence to commitments is a priority.

No new critical systems have been installed or upgraded during the FY25/26 year.

Preventive Maintenance (PM) tasks are generated automatically, and task tickets are assigned to responsible department/team to execute the maintenance, inspection and testing for the system.

Tickets are annotated and closed after the PM has been successfully completed. Any issues discovered are remediated at the time of the PM when possible. If the technician cannot resolve the issue at that time, a new incident ticket is opened and assigned for resolution.

Upgrades to IT Utility Systems are managed by an assigned project manager within UCDH IT as well as a vendor project manager. UCDH IT and the vendor will work together to ensure the upgrade is performed in accordance with the instructions provided by the vendor.

New or replacement IT Utility Systems are managed by an assigned project manager within UCDH IT as well as a vendor project manager. UCDH IT and the vendor will work together to ensure the new or replacement system installation is performed in accordance with the instructions provided by the vendor.