APPENDIX I - LAC+USC FACILITY IT CONTINGENCY PLAN GUIDELINE

OVERVIEW

Contingency planning is the creation of a plan that will be implemented and realized only if a disaster and/or emergency happens. The disaster and/or emergency that will cause an IT Contingency Plan to occur may be very limited (e.g., loss of a server in LAC+USC) or it may be very large (e.g., loss of an entire system across DHS countywide), causing a loss of network resources or it may have nothing to do with IT (e.g., loss of electricity).

An IT Contingency Plan is made up of many parts. One part focuses on IT- the recovery of systems and the systems' data. Another part focuses on the operation of the business- the recovery of operations to allow the workforce members to continue running its day-to-day business until the disaster and/or emergency is over.

The underlying parts of the IT Contingency Plan are the need to back-up the systems and data on a regular basis. The data that is backed up is necessary to recover IT systems and its business operations.

The first step is an analysis of application and data criticality. This allows for information from the LAC+USC Master Security Management Report and prioritizes the sequence in which it will recover systems and data in the event a disaster and/or emergency occur. The template that follows allows for the development of an IT Contingency Plan.

The second step is the Data Backup Plan development. This step determines the quantity and type of information to be backed up so in the event of a disaster and/or emergency the necessary systems and data are restored. It also provides information on the media used, the location of the backups, and the person responsible for each backup.

The third step is the Disaster Recovery Plan development. This is the IT part that identifies the data that will be recovered in the event of a disaster and/or emergency and prioritizes the order in which recovery of systems and information will be conducted. It provides directions on how far in the past to recover data, the time period during which information must be recovered and any specific critical events or time periods during which specific types of information or systems may be needed.

The fourth step is the Emergency Mode Operation Plan development that will allow to appropriately deliver services during a disaster and/or emergency. Regardless of the scope of the emergency, the Emergency Mode Operation Plan provides for emergency operations. If the emergency is limited to a server failure, the emergency mode operation plan may provide direction to use another server somewhere in the Network. If it is a network-wide emergency, the emergency mode operation plan may require operations be performed from another facility until the disaster/emergency is over.

The final steps of the IT Contingency Plan focus on command and control, testing, and workforce IT Contingency Plan training for users. Command and control provide the administrative directions in the event an emergency or disaster occurs. Testing provides for periodic review of the Plan to ensure availability of the necessary systems and data in the event

of a disaster and/or emergency. Workforce member training focuses on preparing designated workforce members to operate the IT Contingency Plan as required.

INSTRUCTIONS

LAC+USC IT Contingency Plan Guideline, below, provides the necessary templates for Information Technology Management to create Contingency Plans to be followed in the event of fire, vandalism, systems failure or other disaster to: (1) recover from the disaster and (2) to continue business operations.

The Chief Executive Officer (CEO) and other designated executive staff must provide oversight and approval for the prioritization of the critical data and Information Systems to ensure that the ranking reflects the Department's critical business functions.

The network CIO/designee must ensure that an IT Contingency Plan containing the following components is created, implemented, tested, and updated for LAC+USC.

All IT Contingency Plans including the components identified below must be provided to the LAC+USC Departmental Information Security Officer (DISO) for review and approval to ensure that the minimum IT Contingency Plan-requirements are met.

LOS ANGELES DEPARTMENT OF HEALTH SERVICES
LAC+USC Medical Center

DATE:

Section 1 LAC+USC Application and Data Criticality Analysis

In this section, LAC+USC Medical Center can leverage the work it did during the Risk Analysis/Management process. Open LAC+USC Master Security Management Report as an Excel spreadsheet. Highlight the columns: Official System Name, System Acronym, System Owner, Information Security Level, Criticality Score, Sensitivity Score, and CEO or designee Priority Level. Copy these columns and paste them into a spreadsheet titled Application and Data Criticality Analysis.

The Network Chief Executive Officer (CEO) or other designated executive staff, must prioritize the systems based on a prioritization of the system functions. The Network CIO must determine the priority of systems for the purpose of this IT Contingency Plan based on the Network Chief Executive Officer or other designated executive staff prioritization and the criticality and sensitivity scores of systems and applications. The priority is as follows:

LAC+USC APPLICATION AND DATA CRITICALITY ANALYSIS TEMPLATE
Date:

Official System Name	System Acronym	System Owner	Information Security Level	Criticality Score	Sensitivity Score	CEO/DIRECTOR Priority Level

Section 2 Data Backup Plan

In this section, the network can copy the Official System Name, Information Technology Management, and CEO/DIRECTOR Priority Level columns from the Application and Data Criticality Analysis. LAC+USC Medical Center can then add a column for Data Backup Method, Data Backup Material, Frequency of Backup and Responsible Person to the spreadsheet to create LAC+USC Data Backup Plan form.

In the column, "Data Backup Method", include the corresponding data backup method (e.g., full, incremental, or differential backup) for each system identified. In the column, "Data Backup Material", include the materials used to create the data backups (e.g., CD-ROM, magnetic tape, or floppy disks. In the column, "Frequency of Backups", include the frequency (e.g., daily, weekly, monthly, and quarterly). Also identify the person(s) responsible for performing, cataloging, inspecting, storing and securing the backups.

The Information Technology Management for each LAC+USC system listed below must ensure the backup of electronic information as provided; the maintenance of those backups; and, offsite storage of the backups. The backups will allow for full system restoration in the event of an emergency.

LAC+USC FACILITY DATA BACKUP PLAN TEMPLATE **Date:**							
Official System Name	System Manager Owner	CEO/DIRECTOR Priority Level	Data Backup Method	Backup Material	Frequency of Backup	Location of Backup	Responsible Person

Section 3 Disaster Recovery Plan

Disaster recovery focuses on the recovery of electronic record and data sets. In this section, the network can copy the Official System Name, Information Technology Management, and the CEO or designee Priority Level columns from the Application and Data Criticality Analysis. The network can then add a column to the spreadsheet for Record and Data Sets to be Recovered, Recovery Point Objective, Recovery Time Objective, and Critical Timeframe to create LAC+USC Disaster Recovery Plan form.

In the Record and Data Sets to be Recovered column, list the record and data sets to be recovered in the event of a loss for each system. A system may have one or more record and/or data sets. For example, a pharmacy system may have a formulary record set, a patient master record set, prescription refill data records, new prescription records, etc. It is important for disaster recovery purposes to identify for each system all electronic record and data sets that LAC+USC intends to recover in the event of loss of the information.

In the next three columns, the Recovery Point Objective identifies the period of time before the outage to which data is to be restored; the Recovery Time Objective identifies the period of time to allow for recovery of the data; and, the Critical Timeframe identifies the time that is critical to have the data recovered.

The Information Technology Management for each LAC+USC system below must be responsible for the recovery of record and data sets from the Point Objective forward. The recovery must occur within the Time Objective and will, whenever possible, meet the Critical Timeframe of the business unit.

LAC+USC FACILITY DISASTER RECOVERY PLAN TEMPLATE **Date:**						
Official System Name	System Owner	CEO/DIRECTOR Priority Level	Record and Data Sets To Be Recovered	RPO[1]	RTO[2]	Critical Timeframe[3]

1. RPO Recovery Point Objective- A measurement of the point prior to an outage to which data are to be restored
2. RTO Recovery Time Objective- The amount of time allowed for the recovery of the record or data source
3. Critical Timeframe- The time that is critical to have the records and/or data restored

Approved 10/30/20
Revised 2/11/14; 9/22/17

Section 4 Emergency Mode Operation Plan

Emergency operation mode focuses on the recovery of operations and business continuity rather than recovery of electronic record and data sets. Some electronic records and data sets may have to be recovered to permit the continuity of operations.

In this section, the network can copy the Official System Name, Information Technology Management, and CEO/DIRECTOR Priority Level columns from the Application and Data Criticality Analysis. The network can then add a column to the spreadsheet for Scope of Emergency, Type of Recovery, LAC+USC Access and System Access to create the Emergency Mode Operation Plan.

The scope of the emergency defines the breadth and extent of the emergency. It may be a system emergency (e.g. loss of mainframe, server, client, or peripheral device like router, switch, hub, or printer); a facility emergency (e.g. loss of a room, floor, loss of utility services to a building or group of buildings on the campus); a LAC+USC emergency (e.g. loss of an enterprise wide application, networking infrastructure, communication infrastructure); or, a County emergency (e.g. a loss of countywide electricity, telephone or other communications).

The type of recovery defines both the locations and recovery methods. An actual location or specific system location will be specified (e.g. Hot site- High Desert; disk mirroring- SS1_Server-Harbor).

A continuity location is the place that can use to recover operation(s) in the event of an emergency or disaster. An internal site is a continuity location within LAC+USC / DHS or the County. An external site is a location that does not belong to LAC+USC / DHS or the County. Examples of the types of locations and data recovery methods are:

Continuity Locations

A hot site is a data center that is configured with the hardware and network communications required to recover operations. The location must be environmentally controlled and available upon a declaration of disaster.

A warm site is a data center that contains HVAC, electrical power, network communication for voice and data access and some hardware available to use for recovery.

A cold site is a data center equipped with HVAC, electrical power and network communications for voice and data. A cold site has no hardware available to use for recovery

LAC+USC EMERGENCY MODE OPERATION PLAN TEMPLATE
Date:

Official System Name	Information Technology Management	CEO/DIRECTOR Priority Level	Scope of Emergency	Type of Recovery	LAC+USC Access	System Access

Data Recovery Methods

Electronic vaulting writes backup tapes over the network to the recovery site. The recovery point objective is shortened because the data that is used is more current than the standard 24 hour-off-site storage process.

Electronic journaling writes transactions and journals over the network to a second location. The information can then be restored on other systems at a hot site. This process diminishes the amount of data lost in the event of an emergency at LAC+USC.

Disk shadowing and mirroring allows for data replication to remote disks. Shadowing is asynchronous, there is a lag between the primary system and the replaced system. Synchronous mirroring means the data sent to the secondary system is current with the primary system.

A hot standby is a replicated server waiting to take the processing load. The hot standby may be load balanced between the primary operating site and a second location to ensure both systems are up-to-date.

The columns titled "Facility Access" and "System Access" require a Yes or No notation. For each type of recovery, "Yes" means that secure access for emergency personnel has been provided to both the network and system recovery site or method.

Emergency operation modes are described by levels depending on the magnitude of the emergency.

Level 1- Emergency Operations- Local day-to-day involving the loss of a location or function

Level 2 Emergency Operations- An incident affecting multiple locations or functions

Level 3- Emergency Operations- Major disruption to one or more locations or functions

Section 5 IT Contingency Plan Command and Control

In this section, the network can copy the Official System Name, Information Technology Management, and CEO/DIRECTOR Priority Level columns from the LAC+USC Medical Center Application and Data Criticality Analysis. The network can then add a column to the spreadsheet for Command Center, Location of Call Tree, Location of Emergency Personnel List and Emergency Access Rights.

The Command Center reflects the place or places the network will use as a command center in the event of an emergency. The LAC+USC Medical Center may have multiple centers in place depending on the scope and extent of the emergency (e.g. a location within the Medical Center, a location within DHS, a location within the County). The location of the list(s) containing the Call Tree including the Emergency Personnel to be called in the event of an emergency should be identified so that one can quickly initiate the Contingency Plans that have been developed. The

column "Emergency Access" requires a "Yes" notation to assure that emergency access rights have been established for emergency personnel.

LAC+USC FACILITY COMMAND AND CONTROL PLAN TEMPLATE **Date:**						
Official System Name	System Owner	CEO/DIRECTOR Priority Level	Command Center	Location of Call Tree	Location of Emergency Personnel List	Emergency Access Rights

Section 6 Test Plan

In this section, the network can copy the Official System Name, Information Technology Management, and CEO/DIRECTOR Priority Level columns from the Application and Data Criticality Analysis. Then the network can then add a column to the spreadsheet for Test Name, Test Location, Plan Cross Reference and Type of Test.

LAC+USC TEST PLAN TEMPLATE **Date**:						
Official System Name	System Owner	CEO/DIRECTOR Priority Level	Test Name	Test Location	Plan Cross Reference	Type of Test

The Test Name is the descriptor that identifies a particular test within the test plan. The Test location identifies where the test preparation worksheet for the particular test is located. The Plan Cross Reference identifies the part or parts of the IT Contingency Plan that the test is intended to measure. The Type of Test describes the kind of test that is being proposed (e.g. checklist test, simulation test, parallel test).

Section 7 Test Plan

In this section, LAC+USC Medical Center can provide a narrative describing its workforce IT Contingency Plan training for designated workforce members, as necessary.