DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Office of Information Services (OIS)
Enterprise Architecture and Strategy Group (EASG)

CMS INFORMATION SECURITY (IS) APPLICATION CONTINGENCY PLAN (CP) PROCEDURES

Version 1.0- FINAL
November 14, 2008

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The *Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Application Contingency Plan (CP) Procedures*, version 1.0, dated September 8, 2008, has been developed as required under the Office of Management and Budget (OMB) Circular A-130*, Management of Federal Information Resources*, *Appendix III,* November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a) (7*)*, which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

The *CMS IS Application Contingency Plan (CP) Procedures* here after known as "CP Procedures" is promulgated under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled *"Contingency Planning Guide for Information Technology Systems"* dated June 2002. The completion of a CP applies to all CMS applications except where an application is included as part of a General Support System (GSS) CP and/or GSS Disaster Recovery Plan (DRP). The Business Owner of every application within the CMS enterprise is required to ensure that a CP is implemented and maintained to reduce risks to reasonable and appropriate levels and to comply with business continuity priorities, applicable laws, regulations, and policies.

The CP Procedures have been developed to serve as a guide for Business Owners and System Developers/Maintainers to develop a CP that will help them to quickly determine the appropriate actions to be taken due to an interruption of service or disaster. The CP Procedures provide a specific format for developing an application level CP and instructions on its content. Utilizing the CP Procedures shall result in a standardized approach to the development of application CPs across the CMS enterprise.

To manage a risk-based IS program, Business Owners and System Developers/Maintainers are responsible for executing the processes defined in the CMS IS Program, such as:

- *CMS Information Security (IS) Certification and Accreditation(C&A) Program Procedures;*
- *CMS Information Security Risk Assessment (IS RA Procedures);*
- *CMS Information Security (IS) System Security Plan (SSP)Procedures;*
- *CMS Information Security (IS) Contingency Plan (CP) Procedures; and*
- *CMS Information Security (IS) Assessment Procedures.*

CMS-CIO-POL-SEC02-3.1, *CMS Policy for the Information Security Program (PISP),* dated June 25, 2008, specifies that all major CMS information systems shall be covered by a CP, relative to the system security level, providing continuation of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption. Designated officials within the organization shall review and approve the CP and **distribute copies of the plan to key contingency personnel.**

Note: - *The CP Procedures and associated template is applicable for CMS Applications only. All CMS GSS' must follow the guidance as specified within NIST SP 800-34.*

1.2 SCOPE

The CP Procedures are focused on the application and its related functions that support or interact with other applications. The CP Procedures apply to the functions, operations, and resources necessary to restore and resume the application after an interruption of service or disaster has occurred. The CP Procedures will designate what equipment, software, hardware and resources are necessary to recover and restore the application at the primary or designated recovery site. The CP Procedures address requirements, preparations, and steps necessary to restore business functions and all of the application components. Many functions and facilities that would be needed in a disruption or disaster involving physical devastation are outside of the current scope of this plan. However, the Business Owner of the GSS supporting the application must include the necessary information in their disaster recovery processes that support the restoration of the application at the appropriate time in the case of a physical devastation.

An application CP shall detail the steps necessary to fully restore and recover the operation of the application in the event of a disruption. The following objectives/processes have been established:

- Maximize the effectiveness of contingency operations through an established plan;
- Identify the activities, resources, and procedures needed to carry out the application during prolonged interruptions to normal operations;
- Assign responsibilities to designated CMS personnel and provide guidance for recovering the application during prolonged periods of interruption to normal operations;
- Ensure coordination with other CMS staff who will participate in the contingency planning strategies for the application; and
- Ensure coordination with external points of contact and vendors who will participate in the recovery and/or restoration of the application.

The CP Procedures are consistent with the PISP and NIST SP 800-53, *Recommended Security Controls for Federal Information System*. The scope/applicability of the application level CP is further depicted in the table below. The application level CP area of applicability are designated in the column under applications - (APP) where in contrast, a GSS level CP would include all CP controls as the GSS level system applicability encompasses all CP controls as delineated in the GSS column.

TABLE 1: APPLICATION CP SCOPE/APPLICABILITY

PISP	NIST SP 800-53	Controls	APP	GSS
4.6.1	CP-1	Contingency Planning Policy and Procedures	●	●
4.6.2	CP-2	Contingency Plan	●	●
4.6.3	CP-3	Contingency Training	●	●
4.6.4	CP-4	Contingency Plan Testing and Exercises	●	●
4.6.5	CP-5	Contingency Plan Update	●	●
4.6.6	CP-6	Alternate Storage Site	---	●
4.6.7	CP-7	Alternate Processing Site	---	●
4.6.8	CP-8	Telecommunications Services	---	●
4.6.9	CP-9	Information System Backup	---	●
4.6.10	CP-10	Information System Recovery & Reconstitution	---	●

The Business Owner and/or System Developer/Maintainer shall coordinate with the related data center to perform the functions and activities associated with Telecommunication Services, Information System Backup, and Information System Recovery & Restoration. The Business Owner is responsible for communicating the backup, recovery, and restoration requirements required to support the application at the data center or its alternate recovery site.

1.3 ROLES AND RESPONSIBILITY

The following roles are responsible for various tasks, assignments, and deliverables throughout the CP Program:

TABLE 2: ROLES AND RESPONSIBILITIES

Role	Responsibility
CHIEF INFORMATION OFFICER (CIO)	The CIO is responsible for, but not limited to, the following: • Ensures a CP is implemented for all CMS GSS and MA to assist in safeguarding assets in the event of a disruption or disaster; • Ensures the CP is part of the C&A package to support the accreditation decision; and • Assists Business Owners in understanding their security responsibilities and ensuring that they incorporate an acceptable level of protection for all CMS IT Systems.
CHIEF INFORMATION SECURITY OFFICER (CISO)	The CISO is responsible for, but not limited to, the following: • Develops and implements IS training that will assist Business Owners and System Developers/Maintainers in the development of the application CP; and • Develops, evaluates and provides information about the CMS IS Program, and communicating CMS IS Program requirements and concerns to CMS management and personnel.
INFORMATION	The ISSO/SSO is responsible for, but not limited to, the following:

Role	Responsibility
SYSTEM SECURITY OFFICER (ISSO)/SYSTEM SECURITY OFFICER (SSO)	• Collaborates with the Business Owner and the System Developer/ Maintainer to ensure internal system controls conform to CMS CP Procedures; • Serves as liaison between the CISO, the System Developer/Maintainer and the Component ISSO/SSO; • Provides technical input to the CP; and • Certifies that the implemented internal system controls are adequate to meet CMS policy and CP Procedure requirements by signing the CP.
BUSINESS[1] OWNER	The Business Owner is responsible for, but not limited to, the following: • Oversees, incorporates, and monitors IS of the assigned application and all related IS artifacts; • Ensures the preparation of the CP including supporting appendices; • Certifies that the implemented internal system controls are adequate to meet CMS policy, standards and CP Procedures by signing and approving the CP; • Selects the Contingency Plan Coordinator (CPC) and oversees the Coordinator's performance; and • Communicates application requirements for recovery, restoration, and reconstitution to the appropriate data center.
SYSTEM DEVELOPER/ MAINTAINER	The System Developer/Maintainer is responsible for, but not limited to, the following: • Incorporates internal controls into the application in consultation with the Business Owner; • Prepares the CP including supporting appendices; • Certifies that the implemented internal system controls are adequate to meet CMS policy, standards and CP Procedures by signing and approving the CP; and • Communicates application requirements for recovery, restoration, and reconstitution to the appropriate data center.
CONTINGENCY PLAN COORDINATOR (CPC)	The CPC is responsible for, but not limited to, the following: • Performs the lead functions to coordinate the recovery, restoration and reconstitution of the application when a disruption of service has occurred.

1.4 DISASTER DEFINITION

For purposes of this CP Procedure, a disaster is any unplanned event that prevents the proper functioning of the application. This definition is derived from CMS' *Information Technology Contingency Plan (ITCP)* and is referenced in the *CMS Master Security Plan* and *CMS Data*

[1] The Business Owner is equivalent to the Information System Owner role as defined by NIST and the Department.

Center GSS System Security Plan (SSP). Both of these documents are stored with the OIS EASG. There are three different disaster types--A, B, C--that exist and are further defined below:

1.4.1 DISASTER TYPE A

This type of disaster is the lowest priority and generally involves an outage of three calendar days or less. This type of disaster may include power failure or unexpected shutdown of the application systems, or a bug in the application code. The data center would not be physically damaged or rendered inoperable. The problem could be corrected with minimal resources. None of the teams may require notification.

1.4.2 DISASTER TYPE B

This type of disaster is one that involves an outage of more than three calendar days but less than seven calendar days. The cause could be a power failure, equipment failure, or damage to the data center. Some or all of the teams may require notification, but mobilization to the hot site probably would not be invoked.

1.4.3 DISASTER TYPE C

This type of disaster will render most of the data center equipment inoperable for at least seven calendar days or more. This type of disaster may include flood, fire, or other significant natural or man made disaster. Once a Type C Disaster is declared, mobilization to the Hot Site facility will be required.

1.5 CP TESTING AND EXERCISES

The Business Owner and System Developer/Maintainer shall establish criteria for validation/testing of a CP, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan’s execution. At a minimum the CP shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. CPs for all application systems must be tested at a minimum using the table top testing process. However, if the application system CP is included in the technical testing of their respective GSS that technical test will satisfy the annual requirement.

1.5.1 TABLETOP TESTING

Tabletop Testing should be conducted in accordance with the *CMS Contingency Planning Tabletop Test Procedures.* The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis; and
- Crisis communications and call tree verification.

1.5.2 TECHNICAL TESTING

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch voice and data telecommunications to alternate processing site.

1.6 CONTINGENCY PLANNING WITHIN THE C&A PROGRAM AND CMS LIFE CYCLE FRAMEWORK

The CP is an integral part of the CMS Certification & Accreditation (C&A) Program and the CMS Integrated IT Investment & System Life Cycle Framework. Typically the CP is executed during the Operations & Maintenance (O&M) Phase of the CMS life cycle. As an application is progressing through the CMS C&A Program, the CP supports the Maintenance, Re-Certification and Re-Accreditation phases. The life cycle, depicted in Figure 1, CMS C&A Phases and Life Cycle Framework, begins with project initiation and ends with system disposition. Although contingency planning is associated with activities occurring in the O&M Phase, contingency measures should be identified and integrated at all phases of the application life cycle. The approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented. Contingency planning is a process that is ongoing throughout the application's life cycle. It should be maintained such that it is current and will be effective in case of a disruption or disaster where a significant loss of service occurs. A further breakdown of when the CP is viewed in the Life Cycle Framework is as follows:

- Planning Stage: The CP is considered when the priority of the application functions have been defined and sequence and requirements to restore the services in the event of a disaster or disruption;
- Requirements Analysis Stage: The CP is considered when the requirement for appropriate system failover capability, data protection, backup, and recovery are defined;
- Implementation Stage: The CP should be one of the deliverables identified in the project plan for implementing the system; and
- Operations & Maintenance: The CP is finalized and certification of its testing is signed by the Business Owner. A signed CP test is needed in order for the system to be accredited the first time. Periodic review is required whenever there are environmental and operational policies or regulatory changes that substantially affect the system.

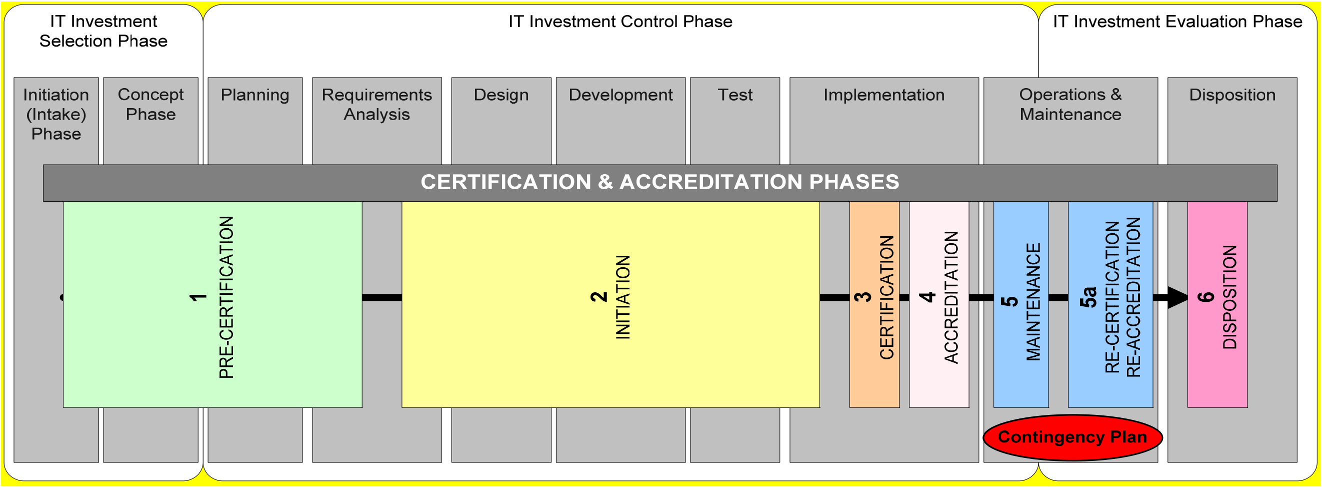

FIGURE 1: CMS C&A PHASES AND CMS LIFE CYCLE FRAMEWORK

1.7 CONTINGENCY PLAN DEVELOPMENT

This section discusses the key elements that comprise the CP. The Business Owner and/or System Developer/Maintainer are responsible for adhering to the procedures delineated in this section and apply appropriate tailoring to support the application. The *CMS Information Security (IS) Contingency Plan (CP) Template, version 2.0, dated September 8, 2008*, corresponds to the CP Procedures and this section and should be used to develop a CP for the respective application. The Business Owner and/or System Developer/Maintainer shall include the five main components of the CP which includes supporting information, notification/activation, recovery, reconstitution, and plan appendices. A summary of the five main CP components is as follows:

1. Supporting Information:
    - Introduction section
    - Concept of Operations section
2. Notification/Activation:
    - Notification procedures
    - Damage assessment procedures
    - Plan activation procedures
3. Recovery:
    - Sequence of recovery activities
    - Recovery procedures
4. Reconstitution:
    - Restore to original sites

- Test systems
- Terminate operations

5. Application CP Appendices:
    - Contact list – Appendix A
    - Vendor Contact list – Appendix B
    - Equipment and software specifications – Appendix C
    - Service level agreements – Appendix D
    - Line of succession – Appendix E
    - Damage assessment – Appendix F
    - Vital records – Appendix G
    - Current configuration – Appendix H
    - Certification – Appendix I

The CP shall contain a Review Log located as the first page behind the cover page. As the CP is required to be reviewed annually (within 365 days), the Review Log captures the date of the reviews, staff reviewers by name/organization, signifying agreement of when and who performed the review. The Review Log shall be maintained to record the reviews that have taken place. The Review Log may be completed by using a pen to write in the data. The CP Review Log shall contain in tabular format the following:

- Date of the reviews;
- Staff name of the reviewer;
- Staff reviewer's organization; and
- CP Version reviewed.

The Business Owners and System Developer/Maintainers shall utilize the CP Template to create their respective application CP. A summary description of each section of the CP is provided in the sections that follow:

2. CP INTRODUCTION SECTION

The CP shall contain an introductory section. The introduction includes background and contextual information that makes the CP easier to understand, implement, maintain and to orient the reader to the information contained in the plan. The introduction should include an overview, scope, roles and responsibilities, assumptions, and record of changes.

2.1 OVERVIEW SECTION

The overview section summarizes the procedures and responsibilities for Notification, Activation, Recovery, and Restoration of the application.

2.2 SCOPE SECTION

The scope section includes the identification of the application to which the CP will cover and the associated subcomponent applications as necessary. The scope details the relationship of the application CP to any other plans supporting or supported by the plan, such as other Disaster Recovery Plans and Emergency Management Plans, etc.

2.3 ROLES AND RESPONSIBILITIES SECTION

This section describes the roles and responsibilities that support and participate in the application's notification/activation, recovery, and reconstitution CP processes. The Business Owner is responsible for ensuring the necessary resources are in place to support contingency planning functions during normal operations and when an incident occurs. The roles and responsibilities for various task assignments and deliverables throughout the contingency planning process are depicted in the table below. It should be noted that the responsibilities listed are suggested and **must** be tailored for each individual application.

TABLE 3: ROLES AND RESPONSIBILITIES

Role	Responsibilities
BUSINESS OWNER – Normal Operations	The responsibilities of the Business Owner during normal operations is as follows: • Develop and maintain the CP no less than every 365 days with review for updates, or when there is a major change to the application/system; • Ensure the required testing of the plan is performed in accordance with the CP testing requirements no less than every 365 days; • Ensure team members that support the recovery effort are trained and have a copy of the CP; • Review plan deficiencies in a timely manner; • Investigate recovery options, develop and implement recovery; solutions, and seek the appropriate funding; • Determine and manage agreements for off-site storage and alternate operating facilities; • Ensure that all recovery team personnel consider recovery preparedness a part of their normal duties and accountabilities; and • Ensures that a copy of the application CP is provided to all identified Key Personnel and must be maintained at an off-site location.

Role	Responsibilities
BUSINESS OWNER – Disruption Occurs	The responsibilities of the Business Owner when a disruption occurs are listed but not limited to the following: • Contact the team members or escalate to senior management depending on the extent of the disaster; and • Delegate responsibility to recovery team members and other CMS personnel.
SYSTEM DEVELOPER / MAINTAINER	The responsibilities of the System Developer/Maintainer are listed but not limited to the following: • Determine the level or type of disaster when incident occurs; and • Determine the extent of response and recovery actions to be performed.
CONTINGENCY PLAN COORDINATOR (CPC)	The responsibilities of the Contingency Plan Coordinator are listed but not limited to the following: • Oversee CP process and CP testing; • Communicate application sanitization requirements for recovery/restoration site; and • Depending on the disaster type or level, coordinate through Disaster Recovery (DR) Management Team who will work with Emergency Management on damage assessment process.
INFRASTRUCTURE SUPPORT / DATA CENTER	The responsibilities of the Infrastructure Support/Data Centers are listed but not limited to the following: • Restore applications at the primary or alternate recovery site; • Recover original application processing functions (if possible within the targeted recovery windows) at the CMS primary site; and • Ensuring sanitization of recovery/restoration site.

2.4 ASSUMPTIONS SECTION

This section discusses the issues, situations, and conditions addressed and not addressed in the CP. The assumptions/constraints when developing the application CP are identified in this section. This section includes an identification of assumption relating to the recovery, restoration, and reconstitution of the application as performed by the data center and within the requirements of the application. The types of contingency situations the plan is intended to cover should be discussed. These situations may range from a temporary loss of commercial power to disaster recovery operations. The system location(s) for the system or system components covered, and any assumptions are described.

- The Business Owner in coordination with the System Developer/Maintainer shall document the relevant assumptions/constraints when developing the application CP. For understanding purposes only, some examples of assumptions/constraints are listed as follows: The application is considered inoperable if it can not be recovered within four (4) hours;

- Key personnel have been identified and trained and are available to activate the application CP;
- Current backups of the application software and data are intact and available at a quickly accessible storage facility;
- Service agreements are maintained with the application hardware, software, and communications providers to support the emergency system recovery;
- Does not include overall recovery and continuity of business operations;
- Does not include emergency evacuation of personnel; and
- Any additional assumptions should be added to this list.

2.5 RECORD OF CHANGES SECTION

This section describes the record of change history of the CP. The Business Owner and System Developer/Maintainer are responsible for ensuring an accurate account for each change to the application CP following its initial release. The Business Owner must sign the Certification of Completion located in Appendix I of the CP to certify the initial completion of the CP. The Record of Change section shall contain in tabular format the following:

- Application identifier;
- Application CP version number;
- Release date;
- Summary of changes;
- Section number and paragraph number changes; and
- Staff who made/authorized the changes.

3. CONCEPT OF OPERATIONS SECTION

The concept of operations section provides additional information to describe the application and the interdependencies of the application. The concept of operations shall include sections that describe the application description and architecture and interdependencies.

3.1 APPLICATION DESCRIPTION AND ARCHITECTURE SECTION

The Business Owner shall provide a statement describing *each* application, the business processes supported by the application and any interdependencies on other CMS systems/ applications, and a description of the technical environment. The Business Owner and/or System Developer/Maintainer shall utilize the application description from the associated SSP and IS RA documents.

The Business Owner and/or System Developer/Maintainer shall provide a statement of purpose and a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunication connections.

3.2 APPLICATION INTERDEPENDENCIES SECTION

Identify and document all CMS supporting systems or applications that are required and/or support the application (i.e. all other CMS applications that “feed” this application, or that are “fed” by this application shall be documented). Provide details regarding System Interconnection and Information Sharing and complete Appendix H of the application CP template with a Connectivity Diagram showing data flow, the list of interdependencies and a current application configuration table.

In this section, provide the following information concerning the authorization for the connection to other systems or the sharing of information for each interconnection between applications:

- Name of system(s);
- Organization owning the other system(s);
- Type of interconnection (Transmission Control Protocol/Internet Protocol (TCP/IP), Domain Trust, Dial, etc.);
- As applicable, attach the Interconnection Security Agreement (ISA) as an appendix to the application CP; and
- As applicable, attach the Memorandum of Understanding (MOU) as an appendix to the application CP.

3.3 CP NOTIFICATION AND ACTIVATION SECTION

This section addresses the initial actions taken to detect and assess damage due to a disruption to the application. It includes activities to notify recovery personnel, assess system damage, and implement the plan. Depending upon the occurrence of an event that results in the loss or disruption of the application processing capability the CMS Business Owner and/or System Developer/Maintainer has the authority to activate and execute the application CP for recovery efforts.

3.3.1 BUSINESS OWNER AND SYSTEM DEVELOPER/MAINTAINER CHECKLIST SECTION

The Business Owner and/or System Developer/Maintainer shall utilize a checklist to ensure the CP process is completed. This checklist should be completed to include the steps to be taken by the Business Owner and/or System Developer/Maintainer in the event of a disruption. The Business Owner and/or System Developer/Maintainer shall use this checklist as a guideline to expedite the decision making process and execute any activities required to provide immediate response and subsequent recovery from the interruption or disaster. The following checklist contains sample language that should be modified based on the application.

TABLE 4: BUSINESS OWNER/SYSTEM DEVELOPER/MAINTAINER CHECKLIST

Steps	Status
1. Determine the status of the work in progress at the time of the disruption and provide a status update to the customers and management.	
2. Determine preliminary disruption scenario.	
3. Perform damage assessment (Appendix F - Damage Assessment).	
4. For Type B or C scenarios, participate as part of the Disaster Recovery Management and/or the Emergency Management teams during their Damage Assessment and Evaluation.	
5. Review section Appendix H- Current Configuration for a good understanding of the applications / system.	
6. Determine criticality of damaged/destroyed items or components.	
7. Determine the need for disaster declaration if disaster level escalating to Type B or Type C.	
8. Send out notification to appropriate personnel according to the disaster scenario and type.	
9. Use section Appendix A- Contact List, Appendix B-Vendor Contacts to notify and coordinate with the internal or external supports if necessary.	
10. Follow the Recovery Procedures reference in Section 3.4 *(Keep in mind that it is impossible to write up procedures for varied scenarios, so use your judgment when executing the procedures.)*	
11. Provide as needed updates according to the disaster scenario.	
12. Document and monitor all recovery activities.	
13. Resume normal operations.	

3.3.2 NOTIFICATION AND ACTIVATION CHECKLIST SECTION

For each type of disaster (Type A, B, and/or C), document in the checklist the notification, activation and damage assessment process. The following is an example of a checklist:

Example for the notification and activation checklist:

- For a Type A disaster, the Business Owner and/or System Developer/Maintainer is notified of the disruption and conducts a damage assessment;
- Based on the damage assessment, the Business Owner and/or System Developer/Maintainer along with the CPC determine if escalation is needed;
- The Business Owner and/or System Developer/Maintainer notifies all members of the Recovery Team;
- The CP is to be activated if one or more of the following criteria are met:
    - The application will be unavailable for more than four (4) hours; and
    - The disruption or disaster is a Type B or Type C;
- If the plan is to be activated, the CPC is to notify all Team Leaders and inform them of the details of the event and if relocation is required;
- Upon notification from the CPC, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond as necessary; and
- The CPC notifies necessary personnel (via notification procedures) on the general status of the incident.

The notification and activation procedures are documented in the table below -
Note *- The checklist below has sample language that needs to be modified to suit each application.*

TABLE 5: CP NOTIFICATION/ACTIVATION CHECKLIST

Date of Incident		**Time of Incident**	
Type of Incident			
Facility / System / Application or Business Impacted			

Expected Duration	**Type A, B, or C Incident**	Completion Status *(As tasks are completed, initial where indicated)*
< 2 hr	1. Receive report of incident or potential event through pager, telephone notification, etc.	
	2. Review to determine the level of disaster.	
	3. If a Type A disaster, the Business Owners and/or System Developers/Maintainers shall conduct the damage assessment for the application. See Appendix F.	
	4. When it is determined that the disaster is a Type B or C, decide whether to declare a disaster.	

Date of Incident		**Time of Incident**	
Type of Incident			
Facility / System / Application or Business Impacted			

Expected Duration	**Type A, B, or C Incident**	Completion Status *(As tasks are completed, initial where indicated)*
	5. Conduct initial status meeting with the various team leaders.	
2-4 hr	1. Begin activation of the CP for the type of disaster.	
	2. Business Owners and/or System Developers/Maintainers coordinate with the CPC for participation in the recovery efforts.	
	3. Business Owners and/or System Developers/Maintainers to instruct Recovery Team to direct all incident status to the CPC or designated alternate(s).	
	4. Determine the extent of response and recovery actions to be performed.	
	5. Establish frequency of communications with other Recovery Teams to provide support and on-going status of current response and recovery activities.	
	6. Establish frequency of communications with the institutional Emergency Management Teams to provide on-going status of current response and recovery activities.	
	7. Established frequency of communications to keep staff informed of the response and recovery progress.	
> 4 hr	1. Observe all staff behaviors and as needed provide periods of rest and relief to elevate stress and correct inappropriate behavior.	
	2. Authorize resources as needed or requested by Recovery Team.	
	3. Maintain a log of recovery activities (e.g., problems encountered, suggestions for improvements to the plan) of each business function affected.	
	4. Document actions and decisions on a continual basis.	

3.4 DAMAGE ASSESSMENT SECTION

The Business Owner in coordination with the System Developer/Maintainer shall ensure damage assessments have taken place and are documented using the Damage Assessment Checklist. The Business Owner and System Developer/Maintainer must coordinate with Infrastructure Support/Data Center service to complete the Damage Assessment Checklist. The Checklist must be completed in Appendix F: Damage Assessment Checklist, within the application CP document. The damage assessment checklist shall contain the following:

- Cause of the disruption or disaster;
- Potential for additional disruption or damage;
- Area affected by the disruption;
- Status of the infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning [HVAC]);
- Inventory and functional status of IT equipment (e.g., fully functional, partially functional, and non-functional);
- Type of damage to IT equipment or data (e.g., water damage, fire and heat, physical impact, and electrical surge);
- Items to be replaced (e.g., hardware, software, firmware, and supporting materials); and
- Estimated time to restore normal services.

After the damage assessment has been completed the Business Owner should follow the notification and activation of the CP. Key personnel should be contacted based on the line of succession. Contact information for other key personnel shall be documented in Appendix A – Contact List of the CP.

3.5 LINE OF SUCCESSION SECTION

The Business Owner in coordination with the System Developer/Maintainer sets forth a line of succession to ensure that decision-making authority for the CP is uninterrupted. The line of succession represents a listing of staff that will be called upon to make assessments and decisions in the event the Business Owner, primary point of contact, is not available. The CP will identify the next four staff who will assume the responsibility to determine and implement the CP in the absence/un-availability of the Business Owner. The line of succession shall be documented in Appendix E of the CP document. The line of succession shall contain the following:

- Name and title;
- Office location and phone number;
- Home phone number;
- Cell phone number; and

- Email address.

In the event there is a disruption, the Business Owner and/or System Developer/Maintainer with coordination of the CPC must determine whether a disaster declaration is necessary based on the outage duration anticipated and the timing of the disaster. If outage is expected to be less than three (3) calendar days, no declaration of disaster is required. However if outage is expected to be more than three (3) calendar days, the level of disaster is escalated to Type B or Type C and a declaration of disaster is required.

Declaration of disaster implies that the emergency situation has resulted in an environment that will necessitate invoking the recovery process. For a Type B and Type C disaster that occurs at the CMS Data Center, the CIO is responsible for declaring a disaster to ensure the safety of personnel, subsequent to the damage assessment process. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the (in order of succession) Deputy CIO, Director of Enterprise Data Center Group (EDCG) and Deputy Directory EDCG shall function as that authority. The Business Owner and/or System Developer/Maintainer in coordination with the CPC determines and documents in the application CP the authority and successors for a Type B and Type C disaster that occurs outside of the CMS Data Center.

3.6 KEY PERSONNEL SECTION

This section contains an identification of the application CP key personnel contacts. The Business Owner in coordination with the System Developer/Maintainer must maintain a list of contact information for each staff identified as key personnel who will be required for recovery operation in the event of an interruption. The Key Personnel Contact List shall be completed in Appendix A of the CP. The Key Personnel Contact List shall contain in tabular format the following:

- Name of staff;
- Office phone number of staff;
- Home phone number of staff;
- Cell phone number of staff; and
- Email address of staff.

4. RECOVERY AND RESTORATION SECTION

This section describes the procedures for recovering the application. The teams shall follow the procedures as documented within the checklist and in accordance with each group's internal procedures. Recovery activities focus on contingency measures to execute temporary application processing capabilities, repair damage to the original application, and restore operational capabilities at the original or new facility. At the completion of the recovery activities, the application will be operational and performing the functions designated in the plan. The recovery functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. The Business Owner and/or System Developer/Maintainer are responsible for coordinating with the Infrastructure Support/Data Center personnel to ensure the recovery and restoration activities are performed in accordance with the requirements of the application.

4.1 RECOVERY TEAM RESPONSIBILITY SECTION

This CP establishes several teams assigned to participate in the recovery of the operations for the application and their responsibilities for the application when responding to a disruption. The CP shall contain in tabular format a detailed identification of all roles and responsibilities of the various teams for the recovery of the application that includes the following:

- Component/Group/Team - This type of personnel would include database administrators, application developers, infrastructure personnel, etc., that are necessary components for the recovery of the application and a part of the team required during a disruption/disaster;
- Contact Person Name and Title - This is the name of the person who will be contacted to activate the group or team for the recovery efforts;
- Contact Information - This includes the on-site and off-site access contact information for the person cited in the contact person list; and
- Area of Responsibility - This includes the roles and responsibilities of the group/team/person. (For example: a Database Administrator role/responsibility could include installing and restoring the application database which includes software currently available in the live production environment.)

4.2 RECOVERY PRIORITIES SECTION

The Business Owner and/or System Developer/Maintainer shall document the recovery priorities as determined for the application and application sub-components in this section. To determine this information, the Business Owner and/or System Developer/Maintainer shall perform the following:

- Review application documentation that describes the recovery priorities of the application and associated application sub-components;
- Determine application/sub-application criticality based on business operations; and
- Document the recovery priorities.

The application CP priorities for recovery shall be documented in tabular format and contain the following:

- Recovery priority;
- Associated hardware; and

- Associated software.

4.3 RECOVERY PRE-REQUISITES SECTION

The recovery prerequisites are dependent on the type of disruption that occurs and these may be different for different types of scenarios for the application. Before recovery of application can be started, various jobs may be required to be performed or data may need to be available. The Business Owner and/or System Developer/Maintainer shall document all jobs, resources, and data required for the successful restoration of the application. The CP shall cite in tabular form the specific requirements for the application including the following:

- Job name;
- Job frequency;
- Job description;
- Type (A, B, C) recovery prerequisite selected;
- Allowable outage time;
- Cost considerations for being down;
- Cost considerations for restoring operations; and
- Application specific information for documentation required to restore the application.

For example: The following prerequisites are necessary for recovery and restoration based on the type of disaster:

- The Business Owner in coordination with the System Developer/Maintainer will notify users of the approximate down time and up time. Users will be provided with notification when the system is available for use;
- The Business Owner and/or System Developer/Maintainer for the application are required to work together with the Data Center IT Service Desk to restore any lost functionality;
- The Business Owner and/or System Developer/Maintainer will be responsible for restoring any lost or damaged services and will work with the Infrastructure Staff for providing network and other infrastructure services. After the services are restored, the application needs to be initialized. Information for initializing the application is documented in the *System Operations Manual*; and
- In order for the application to be recovered at the Hot Site, system operation manuals, server build documents, operating system documents, equipment, and software are required.

4.4 ALTERNATE STORAGE/PROCESSING SITE AND TELECOMMUNICATION SERVICES SECTION

The Business Owner and/or System Developer/Maintainer are not responsible for Alternate Storage Site, Alternate Processing Site, and Telecommunications Services recovery procedures. The Business Owner and/or System Developer/Maintainer shall refer to the appropriate GSS CP to address these areas. The Business Owner in coordination with the System Developer/Maintainer are responsible for recording the alternate site storage information from the organizations that will carry out this function and documenting the information in the CP.

4.5 INFORMATION SYSTEM BACKUP AND INFORMATION SYSTEM RECOVERY AND RECONSTITUTION SECTION

The Business Owner and/or System Developer/Maintainer shall communicate their respective Information System Backup and Information System Recovery & Reconstitution process requirements that are more stringent then the current processes being performed by the Data Centers. The Business Owner and/or System Developer/Maintainer shall record the Data Centers agreement to alter processing to meet the application's information system backup and information system recovery & reconstitution requirements.

4.6 RECOVERY AND RESTORATION CHECKLIST

The Business Owner in coordination with the System Developer/Maintainer shall use the Application's technical operations document that contains information for restoring any technical and business services related to the application to support recovery of that application. The Business Owner and/or System Developer/Maintainer is responsible for maintaining all necessary documentation used to restore the application and ensure this information is stored off-site from the primary operations location of the application. The Business Owner in coordination with the System Developer/Maintainer documents the application recovery and restoration procedures using a recovery and restoration checklist. The Business Owner and/or System Developer/Maintainer shall document the recovery and restoration checklist information using a tabular format and contain at a minimum the following:

- Application Business Owner or Designated Alternate(s);
- Date of Incident;
- Time of Incident;
- Type of Incident (Type A/B /C) Describe incident;
- Facility / Application or Business Impacted;
- Expected Duration;
- Completion Status *(As tasks are completed, initial where indicated*; and
- Detailed Recovery and Restoration Procedures based on Type of Incident.

5. RETURN TO NORMAL OPERATIONS SECTION

The System Developer/Maintainer shall assist in the return to normal operations in the situation that “bad code” has been determined to be the problem. Otherwise the Infrastructure Support/Data Center personnel shall have responsibility to lead the efforts to return the application to normal operations.

This section shall define the steps necessary to return the application to normal operations. The steps shall define the organizations and associated roles that will take place in order to return the application to normal operation. The CP shall contain the application’s checklist that documents the step by step process. This checklist will also serve to support training and testing/exercising of the application CP. The recovery and restore checklist elements that need to be completed include but are not limited to the following:

- Application Business Owner or Designated Alternate(s);
- Date of Incident;
- Time of Incident;
- Type of Incident;
- Facility, system, application or business impacted;
- Expected duration of the outage and the procedures linked to the duration of outage;
- CP reconstitution/return to normal operations checklist – the procedures to bring the application back to the original site or a new site; and
- Completion status – This column remains blank and shall be completed in the event of an interruption to track the progress of the tasks.

The checklist below includes procedures to operate the system at the original or new site. The procedures include testing the original or new system as documented in the CP, and the steps to clear site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). The disruption is considered over when all of the application components and application sub-components are operational.

<u>Note: -</u> *The checklist below has sample language that needs to be modified to suit each specific application.*

TABLE 7: SAMPLE RETURN TO NORMAL OPERATIONS CHECKLIST

Application Business Owner or Designated Alternate(s)			
Date of Incident		**Time of Incident**	
Type of Incident (Type A/B/C) Describe incident			

Facility / Application or Business Impacted		
Expected Duration to complete	**Disruption**	**Completion Status** *(As tasks are completed, initial where indicated)*
	1. The Business Owner and/or System Maintainer shall coordinate with CIO Office or CPC to determine data and time the restored facility will be available for return.	
	2. The Business Owner and/or System Maintainer determine when transition back to normal operations or recovery may be appropriate, based on status reports and completion of action plans.	
	3. Schedule meeting to terminate response and recovery activities and return to normal operations.	
	4. If hot site was utilized, begin to return to primary site for restoration of application.	
	5. Define status of support services (e.g. telephone, computer services, etc.).	
	6. Coordinate any special logistical requirements or support which will be available to the Recovery Teams (e.g. transportation for equipment and records, assistance with packing records, etc.).	
	7. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s).	
	8. Restore the application to the primary recovery site utilizing a Recovery and Restoration Checklist.	
	9. Conduct operational checks. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.	
	10. Ensure that the recovery site is sanitized of all information after applications returns to normal operations.	
	11. Document lessons learned and update CP.	

6. CP SUPPORT DOCUMENTATION

The Business Owner and/or System Developer/Maintainer are responsible for ensuring CP support documentation is recorded or its name and off-site location are referenced in the CP. The application support documentation should be maintained in the application Configuration

Management Plan or System Configuration documents and under configuration control. The Business Owner and/or System Developer/Maintainer shall include in the CP the support documentation identified below:

6.1 VENDOR CONTACT LIST

The Vendor Contact List contains a listing of the vendors that supported the development of the application and the vendors that will be needed to recover and restore the application in the event of a disruption of service. The Business Owner and/or System Developer/Maintainer shall document the vendor contact information in Appendix B of the CP. The Vendor Contact List shall contain in tabular format the following:

- Vendor name;
- Vendor contact person;
- Reference documentation listing;
- Phone number of vendor contact person; and
- Email address of vendor contact person.

6.2 EQUIPMENT AND SOFTWARE SPECIFICATION

The Equipment and Software Specification contains a listing of the equipment and software baseline that supported the development of the application and maintained under configuration control. The equipment and software specifications will be provided to the vendors and Data Center in order to recover and restore the application to normal operations in the event of a disruption. The Business Owner and/or System Developer/Maintainer shall document the Equipment and Software Specification information in Appendix C of the CP. The equipment and software specification information shall contain in tabular format the following:

- Component/Group;
- Contact Person;
- Area of Responsibility;
- Version of the software
- Version of the hardware; and
- Reference documentation.

6.3 VITAL RECORDS

The Business Owner and/or System Developer/Maintainer shall identify the documents that are considered critical to identifying, restoring, and maintaining the application as a vital record. The vital records for the application shall be maintained in the Appendix G of the CP. The vital records information shall contain in tabular format the following:

- Document name;
- Date and/or version number;
- Media;
- Department; and
- Contact.

6.4 CURRENT CONFIGURATION

The Business Owner and/or System Developer/Maintainer shall document the current configuration information in Appendix H of the CP. The current configuration at a minimum shall contain the following:

- Connectivity diagram or data flow diagram;
- Inter-dependencies/interfaces; and
- Current configuration table.

6.5 CERTIFICATION OF BUSINESS OWNER

The Business Owner shall certify that they have reviewed the CP and that the procedures described in the CP are accurate and are a complete description of the actions to be taken in the event of a disruption of service/disaster. In addition, the Business Owner certifies that the CP has been tested and that all parties involved in the contingency planning process have been informed and accepts their roles and responsibilities and that the processes depicted in the CP can be put into effect as described with the CP. The Business Owner shall document their certification in Appendix I of the CP.

APPENDIX A – ABBREVIATIONS AND ACRONYMS

APP	Application
ARS	Acceptable Risk Safeguards
C&A	Certification & Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CP	Contingency Plan
CPC	Contingency Plan Coordinator
DC	Data Center
DITPPA	Division of Information Technology Policy, Procedures, and Audits
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EASG	Enterprise Architecture & Strategy Group
EDCG	Enterprise Data Center Group
FISMA	Federal Information Security Management Act of 2002
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HVAC	Heating, Ventilation, and Air-Conditioning
IS	Information Security
ISA	Interconnection Security Agreement
ITCP	Information Technology Contingency Plan
MOU	Memorandum Of Understanding
NIST	National Institute of Standards and Technology
OIS	Office of Information Services
O&M	Operations & Maintenance
OMB	Office of Management and Budget
PISP	Policy for the Information Security Program
SDLC	System Development Life Cycle
SP	Special Publication
SSP	System Security Plan
TCP/IP	Transmission Control Protocol/Internet Protocol
TMG	Technology Management Group
ST&E	Security Test & Evaluation
VPN	Virtual Private Network

End of Document