



State Offices, Service
Centers, and Service
Center Agency Partner
Specialty Offices

Office of the Chief Information Officer (OCIO)
Information Technology Services (ITS)
Field Support Contingency Plan

June 27, 2005

**United States
Department of
Agriculture**

For Official Use Only

TABLE OF CONTENTS

1.0	INTRODUCTION	3
1.1	CONTINGENCY PLAN ELEMENTS	3
1.2	PURPOSE	3
1.3	OBJECTIVES.....	4
1.4	SCOPE	4
1.5	ASSUMPTIONS.....	5
1.6	REFERENCES	5
2.0	CONCEPT OF OPERATIONS	7
2.1	ORDER OF SUCCESSION	8
2.2	ROLES AND RESPONSIBILITIES.....	9
2.3	COMMUNICATIONS PLAN	10
3.0	NOTIFICATION AND ACTIVATION PHASE	11
3.1	EMERGENCY CONTACT INFORMATION	12
3.2	LOCATION INFORMATION TEMPLATE	12
3.3	IT DAMAGE ASSESSMENT FORM	12
4.0	RECOVERY PHASE	13
4.1	SYSTEM SHUTDOWN.....	13
5.0	RECONSTITUTION	14
5.1	PLAN DEACTIVATION.....	14
6.0	TESTS, TRAINING, AND EXERCISES	15
6.1	TESTS	15
6.2	TRAINING AND EXERCISES.....	15
7.0	PLAN MAINTENANCE	16
APPENDIX A	EMERGENCY CONTACT INFORMATION	17
APPENDIX B	LOCATION INFORMATION TEMPLATE AND INSTRUCTIONS	19
APPENDIX C	IT DAMAGE ASSESSMENT FORM AND INSTRUCTIONS	23
APPENDIX D	SHORT AND LONG TERM SYSTEM REQUIREMENTS	26
APPENDIX E	RECOVERY DOCUMENTS LIST	28
APPENDIX F	DAILY OPERATIONS LOG	31
APPENDIX G	RECORD OF CHANGES	32
APPENDIX H	DISTRIBUTION LIST	33
APPENDIX I	ACRONYMS	34

1.0 INTRODUCTION

Each agency within the United States Department of Agriculture (USDA) has been instructed to develop Information Technology (IT) contingency plans for the agency's mission critical systems to enable their continuity during and after an emergency in support of their critical business processes. These IT contingency plans are key elements in USDA's overall contingency program, which also includes Disaster Recovery Plans (DRP), and Continuity of Operations Plans (COOP). Together, these plans comprise a comprehensive contingency planning capability.

1.1 CONTINGENCY PLAN ELEMENTS

IT CONTINGENCY PLAN

An IT Contingency Plan is typically developed for each mission critical system within an organization. An IT Contingency Plan should be developed for each mission critical system within an organization that supports the execution of a key business process. For State Offices, Service Centers, and Service Center Agency (SCA) Partner Specialty Offices, a comprehensive contingency plan document, which includes site specific information and IT recovery procedures, is being implemented to support the recovery of essential IT functions. When a disruption to IT functionality occurs, this contingency plan will be activated to provide all the necessary information required to restore IT functions at any State Office, Service Center, or SCA Partner Specialty Office location.

DISASTER RECOVERY PLAN

The Disaster Recovery Plan (DRP) applies to major, usually catastrophic, events that deny access to the normal facility for an extended time period. Frequently, a DRP refers to an IT-focused plan designed to restore operability of target systems, applications, or the computer facility at an alternate site in the event of an emergency.

CONTINUITY OF OPERATIONS PLAN

The Continuity of Operations Plan (COOP), which is a separate document, is developed to aid a department or agency in restoring the organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The COOP typically addresses headquarters-level issues and is executed independently.

1.2 PURPOSE

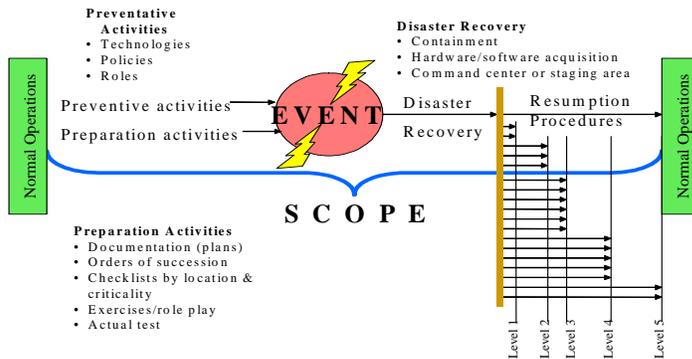
This document, the Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) Field Support Contingency Plan, establishes procedures to recover the essential IT functions and equipment following an event or disruption at State Offices, Service Centers, and SCA Partner Specialty Offices. The appendices of this document also include a form for documenting emergency contact information, a template for collecting site specific information, a damage assessment template, and a list of the recovery documents that will be needed to restore IT functionality following an event or disaster. This contingency plan document provides the complete IT Contingency and Disaster Recovery requirements for each State Office, Service Center, and SCA Partner Specialty office location.

1.3 OBJECTIVES

The following objectives have been established for this plan.

- Maximize the effectiveness of contingency operations through an established methodology that consists of the following phases:
 - Notification/Activation phase* to detect and assess damage and to activate the plan.
 - Recovery phase* to restore temporary IT operations and recover damage done to the original system.
 - Reconstitution phase* to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out State Office, Service Center, and SCA Partner Specialty Office IT functions during prolonged interruptions to normal operations.
- Assign responsibilities to designated personnel and provide guidance for recovering a State Office, Service Center, or SCA Partner Specialty Office IT functionality during prolonged periods of interruption to normal operations.
 1. Ensure coordination with other OCIO-ITS staff who will participate in the IT Contingency Planning strategies.
 2. Ensure coordination with external points of contact and vendors who will participate in the IT Contingency Planning strategies.
 3. Ensure coordination with the Continuity of Operations Plan (COOP) at each State Office, Service Center, and SCA Partner Specialty Office location.

1.4 SCOPE



IT Contingency Plan

07 Jul 03

This plan applies to State Offices, Service Centers, and Service Center Agency (SCA) Partner Specialty Offices as of January 11, 2005. It addresses the site specific contact information, functions, operations, and resources necessary to restore essential IT functionality. The plan also applies to all personnel identified in Section 2.3 with responsibilities associated with the recovery of essential IT functionality at State Offices, Service Centers, and SCA Partner Specialty Offices.

1.5 ASSUMPTIONS

The following assumptions were made when developing this OCIO-ITS Field Support Contingency Plan:

- IT functionality is inoperable and cannot be recovered within 72 hours.
- Designated personnel have been identified and trained in their contingency plan responsibilities and are available to implement the plan.
- Preventive controls such as sprinkler systems and fire extinguishers are operational at the time of the disaster.
- Current backups of the application software and data are intact and available at the off-site storage facility.
- OCIO-ITS staff are available to provide any necessary IT support.
- OCIO-ITS will be able to obtain the equipment needed to recover critical IT functions.
- A Continuity of Operations Plan (COOP) is in place at each State Office, Service Center, and SCA Partner Specialty Office location and addresses the following:
 - Facility – space and cubicles
 - People – business staff
 - Utilities – electricity, gas, water, etc.
 - Office Supplies
 - Vehicles
 - State Office, Service Center, and SCA Partner Specialty Office Vital Records

The State Offices, Service Centers, and SCA Partner Specialty Offices OCIO-ITS Field Support Contingency Plan does not apply to the following:

- Overall recovery and continuity of business operations. The Continuity of Operations Plan (COOP) is a separate document and is the responsibility of the Agency.
- Emergency evacuation of personnel. The Occupant Evacuation Plan (OEP) is a separate document and is the responsibility of site management.

1.6 REFERENCES

This State Offices, Service Centers, and SCA Partner Specialty Offices OCIO-ITS Field Support Contingency Plan complies with applicable Contingency Plan policy as follows:

The organization shall develop a Contingency Planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal Contingency Plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The State Offices, Service Centers, and SCA Partner Specialty Offices OCIO-ITS Field Support Contingency Plan also complies with the following federal and *departmental* policies:

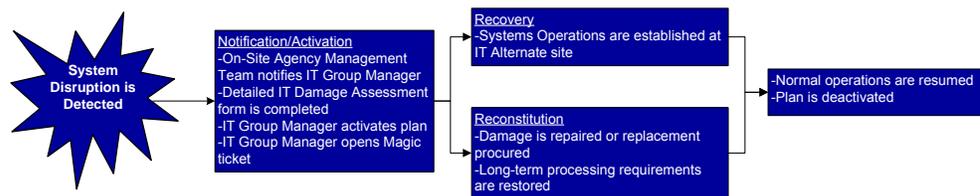
- The Computer Security Act of 1987
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000.
- Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, May 1998
- Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 1998
- Federal Emergency Management Agency (FEMA), *The Federal Response Plan (FRP)*, April 1999
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000
- Department of Commerce National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 *Contingency Planning Guide for Information Technology Systems*, 2001
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations (COOP)*, June 15, 2004

2.0 CONCEPT OF OPERATIONS

Figure 2-1 depicts the IT Contingency Plan implementation strategy. This plan is implemented in the following three phases following a disruptive event:

- **NOTIFICATION AND ACTIVATION PHASE:** After a system disruption is detected, management is notified of the event and makes the decision to activate the plan based on the results of a damage assessment
- **RECOVERY PHASE:** Based on the nature and magnitude of the disruption, temporary system functions are restored at their original site or another location
- **RECONSTITUTION/BUSINESS PROCESS RESUMPTION PHASE:** Concurrent with the recovery phase, actions are taken to restore permanent system operations either at the original site or another location. At the end of this phase, system operations are transferred from the temporary “recovery” system and normal operations are restored to the permanent system.

Figure 2-1 OCIO-ITS Field Support Plan Implementation Strategy



2.1 ORDER OF SUCCESSION

OCIO-ITS has identified an order of succession, in accordance with the order of succession established by the Department, to ensure that decision making authority for the OCIO-ITS Field Support Contingency Plan is uninterrupted. The IT Group Manager is responsible for ensuring execution of the procedures documented within this contingency plan. If the IT Group Manager is unable to function as the overall authority or chooses to delegate this responsibility to a successor, authority will pass to the designated party as indicated below.

**OCIO-ITS Field Support Contingency Plan
Delegation of Authority and
Order of Succession**

MISSION AREA State Offices, Service Centers, and SCA Partner Specialty Offices	
AGENCY OCIO-ITS	
DESCRIPTION In the event of my inability to act as IT Group Manager, during a significant incident, disaster, or emergency requiring activation of the IT Contingency/Disaster Recovery Plan, due to absence, sickness, resignation, or death, provisional authority is hereby delegated to the incumbents of the positions named below to act as IT Group Manager. In the event a permanent appointee has not been appointed, delegation of authority shall follow the line of succession to fulfill this requirement. Each official shall act only in the absence, sickness, resignation, or death of the immediately preceding official. The designees, listed in order of precedence to act, are:	
TITLE	LOCATION
OCIO-ITS Regional Branch Chief	
OCIO-ITS Director, Technical Services Division	Larry Brooks, Fort Collins

2.2 ROLES AND RESPONSIBILITIES

Key OCIO-ITS, State Office, Service Center, and SCA Partner Specialty Office personnel have been identified and trained to ensure the continuity of maintaining, recovering, and restoring essential IT functionality. Table 2-1 identifies the teams required for implementing this plan and their respective responsibilities.

Table 2-1 OCIO-ITS Field Support Contingency Personnel, Teams and Responsibilities

PERSONNEL/TEAMS	RESPONSIBILITIES
IT Group Manager	<ul style="list-style-type: none"> • Has overall responsibility for the event/disaster • Determines if plan activation is necessary • Determines the scope of plan implementation • Opens Magic ticket to OCIO-ITS support staff for distribution to appropriate support teams (AS/400, CCE, Telecom, etc.) • Maintains contact information for OCIO-ITS support personnel (not listed in plan) • Reports the status of the situation to OCIO-ITS management and Agency management on a daily basis. • Completes all incident documentation (Status reports, After Action reports, etc.)
On-Site Agency Management Team	<ul style="list-style-type: none"> • Notifies IT Group Manager of event • Completes IT Damage Assessment Form (Appendix C) with State/County Emergency Board • Activates the Continuity of Operations Plan (COOP) if necessary • Updates IT Group Manager of status as needed
AS/400Team	<ul style="list-style-type: none"> • Receives Magic ticket indicating the nature and scope of the system disruption • Contacts State and Local OCIO-ITS Support Team to begin recovery process • Coordinates AS/400 recovery procedures with FSA staff • Coordinates activities with other OCIO-ITS Teams for all affected systems • Provides status updates to the IT Group Manager as requested
CCE Team	<ul style="list-style-type: none"> • Receives Magic ticket indicating the nature and scope of the system disruption • Contacts State and Local OCIO-ITS Support Team to begin recovery process • Initiates CCE recovery procedures • Coordinates activities with other OCIO-ITS Teams for all affected systems • Provides status updates to the IT Group Manager as requested
Telecom Team	<ul style="list-style-type: none"> • Receives Magic ticket indicating the nature and scope of the system disruption • Contacts State and Local OCIO-ITS Support Team to begin recovery process • Initiates Telecom recovery procedures • Coordinates activities with other OCIO-ITS Teams for all affected systems • Provides status updates to the IT Group Manager as requested
State and Local OCIO-ITS Support Team	<ul style="list-style-type: none"> • Assists in completing the IT Damage Assessment Form • Oversees, maintains, and ensures the recovery of their assigned systems and support components • Works with various OCIO-ITS teams to recover and/or repair affected system(s) • Reports system(s) status to IT Group Manager as requested

Note: While State and Local OCIO-ITS support teams will be involved in on-site recovery, other OCIO-ITS teams may work remotely to recover IT functionality.

2.3 COMMUNICATIONS PLAN

Throughout plan activation, the IT Group Manager will maintain a daily operations log (Appendix F). The log will contain status information from the On-Site Agency Management Team, the State and Local OCIO-ITS Support Teams, and any other participating OCIO-ITS Support Teams (AS400 Team, CCE Team, and Telecom Team). The IT Group Manager will provide a status report to OCIO-ITS Management and Agency Management on a daily basis. Figure 2-2 illustrates the Communication Plan Strategy.

Figure 2-2 Communications Plan Strategy



3.0 NOTIFICATION AND ACTIVATION PHASE

The Notification and Activation Phase identifies the initial actions taken to detect and assess the damage inflicted by an event or disaster at a State Office, Service Center, or SCA Partner Specialty Office location rendering essential IT services non-functional. Contact information for key personnel is documented in Appendix A.

After being notified of a system disruption, the ITS Group Manager works with On-Site Agency Management and State and Local OCIO-ITS staff to assess system status and the extent of damage to determine whether plan implementation is necessary. The IT Damage Assessment Form in Appendix C is completed to assist in this evaluation process. Following a decision to activate the plan, the ITS Group Manager opens a Magic ticket to notify the appropriate OCIO-ITS Support staff. Figure 3-1 depicts the notification and activation process.

Figure 3-1 Notification and Activation Flowchart



The State Offices, Service Centers, and SCA Partner Specialty Offices OCIO-ITS Field Support Contingency Plan is to be activated if one or more of the following criteria are met:

- An event occurs that affects agency operations and is of significant magnitude to require an active disaster recovery effort
- An event occurs that requires resources beyond local capabilities
- A local or state emergency is declared
- Activation of the contingency plan will be advantageous to the successful management of the emergency
- The event causes a disruption to IT functionality that is expected to last beyond 72 hours

Once the plan is activated, the ITS Group Manager notifies the following personnel of plan implementation:

- On-Site Agency Management Team
- OCIO-ITS Support Team Leaders (OCIO-ITS State and Local Support Team, AS/400 Team, CCE Team, Telecom Team)
- OCIO-ITS Management
- Agency Management

3.1 EMERGENCY CONTACT INFORMATION

The Emergency Contact Information form, which can be found in Appendix A, is used to document critical contact information that will be needed when a disruption or disaster occurs. This form is to be completed for each office. Copies of the completed form should be stored off-site, provided to local ITS staff, provided to Agency management, and be available for use in an emergency.

3.2 LOCATION INFORMATION TEMPLATE

The Location Information Template, which can be found in Appendix B, is to be completed for each office. This template is designed to collect site specific information including location of backup tapes, building access, preventive controls, and the IT alternate site location that will be needed when a disruption or disaster occurs. Copies of the completed template should be stored off-site, provided to local ITS staff, provided to Agency management, and be available for use in an emergency.

3.3 IT DAMAGE ASSESSMENT FORM

The detailed IT Damage Assessment Form, which can be found in Appendix C, is to be completed to evaluate damage to critical IT systems following an event or disaster at a State Office, Service Center, or SCA Partner Specialty Office location. This form should be completed by On-Site Agency Management in conjunction with State/County Emergency Board when appropriate.

4.0 RECOVERY PHASE

This phase of the OCIO-ITS Field Support Contingency Plan includes the procedures for recovering IT essential functionality at the IT Alternate Site. A listing of the detailed recovery documents is included in Appendix E of this document. These recovery documents will be available at the CCE Team Services web site (<http://century.itc.nrcs.usda.gov/cce-states/>) for use in an emergency. These documents are hosted centrally, at an off-site location, for all State Offices, Service Centers, and SCA Partner Specialty Offices to utilize. When using any of the recovery documents, each procedure should be executed in the sequence in which it is presented to maintain efficient operations.

Note: A user name and password are required to access the CCE Team Services web site.

4.1 SYSTEM SHUTDOWN

If time permits, the designated personnel should shut down the system gracefully to prevent data corruption, hardware damage, and limit the potential spread of the disruption. Shutting down the system gracefully allows data to remain intact, preventing potential data loss. If the disruption results from the introduction of malicious code, shutting down system components promptly may limit the extent of the code's affects.

The support documents for the various ITS hardware and software that may be found in State Offices, Service Centers, and SCA Partner Specialty Offices are listed in Appendix E and will be available at the CCE Team Services web site. To ensure proper system shutdown, the procedures in these documents should be executed in the sequence in which they are presented in each applicable document.

5.0 RECONSTITUTION

The reconstitution phase includes those activities necessary for restoring IT functionality at the State Office, Service Center, or SCA Partner Specialty Office original site or a new site. When the original location has been restored or a new site has been prepared, IT operations at the alternate site must be transitioned back. The documents listed in Appendix E contain all of the necessary procedures for setting up IT equipment and restoring essential IT functionality at the original or new site.

5.1 PLAN DEACTIVATION

When the IT functionality is recovered and normal operations are resumed, the contingency plan may be deactivated. Final actions that may be required at this stage include returning leased or borrowed equipment or materials; notifying appropriate personnel that system operations are being returned to the primary site; and documenting final actions, adjustments to the plan, and any other pertinent information. Lastly, personnel should be instructed to return to the original or new site.

6.0 TESTS, TRAINING, AND EXERCISES

OCIO-ITS personnel will participate in IT contingency planning test, training, and exercise (TT&E) events to ensure their familiarity with contingency planning activities and their respective responsibilities. These activities help ensure that personnel can respond to system disruptions effectively. Table 6-1 below illustrates the TT&E schedule.

6.1 TESTS

The primary purpose of testing the IT contingency plan is to ensure that the plan is accurate, complete, and contingency personnel are able to perform their recovery/reconstitution procedures accurately and within the designated timeframe. Additional testing may also be required after significant changes in personnel, system operations, or architecture.

6.2 TRAINING AND EXERCISES

For a contingency plan to be implemented successfully, contingency personnel must be trained and able to perform their responsibilities efficiently and accurately. Training and exercise events will be scheduled regularly to provide teams with an opportunity to review and discuss their roles and perform their assigned responsibilities in a simulated emergency environment. New personnel with contingency plan responsibilities will receive a copy of this plan and be trained on its content and their respective responsibilities. Table 6-1 depicts the TT&E schedule.

TABLE 6-1 TEST, TRAINING, AND EXERCISE SCHEDULE

TT&E EVENT	QUARTERLY	SEMIANNUALLY	ANNUALLY
Notification Tests		✓	
Orientation Training	On-going, as needed		
Tabletop Exercises			✓
Functional Exercises	As needed		

7.0 PLAN MAINTENANCE

ITS Group Managers are responsible for completing and maintaining Appendix A (Emergency Contact Information) and Appendix B (Location Information Template) for each location within their group. Copies must be stored off-site, provided to key IT staff for the locations for which they are responsible, and, when requested, provided to Agency Management and OCIO-ITS Management. These documents should be reviewed and updated at least semi-annually and more frequently if major changes occur.

OCIO-ITS-IGD-Security Policy Branch staff will retain responsibility for the overall contingency program to include maintenance of the templates, availability of recovery information via the CCE Team Services web site, and coordination of the TT&E program.

Changes made to this plan are documented in the Record of Changes table in Appendix G. The IT Group Managers and OCIO-ITS-IGD-Security Policy Branch staff will ensure that changes made to this plan are consistent with USDA and OCIO-ITS policy, other plans within the department or agency, and the USDA IT Contingency Plan Maintenance Guide.

APPENDIX A EMERGENCY CONTACT INFORMATION

This appendix provides emergency contact information that State Office, Service Center, or SCA Partner Specialty Office personnel might need following an event or disaster resulting in a system disruption. Please complete the OIP Site Number for the location and the specific contact information indicated (name, street address, e-mail address, office phone, office fax, home phone, and mobile phone) for each contact listed.

Note: Please use the Excel spreadsheet version of this template (see icon at the bottom of this page) to collect the information from each site.

OIP Site Number _____

Name	Title	Street Address	E-mail Address	Office Phone	Office Fax	Home Phone	Mobile Phone
Tom Radermacher	ITS Group Manager	375 Jackson St, Suite 600, St Paul, MN	Tom.Radermacher@mn.usda.gov	651-602-7903	651-602-7914	651-784-5485	None
Pam Howard	ITS Specialist	375 Jackson St, Suite 400, St Paul, MN	Pamela.Howard@mn.usda.gov	651-602-7739	651-602-7743	612-729-4917	None
Rick Killmer	ITS Specialist	375 Jackson St, Suite 400, St Paul, MN	Rick.Killmer@mn.usda.gov	651-602-7788	651-602-7743	651-330-3928	None
	Agency Site Manager						
	Local OCIO-ITS Staff						
	Central Help Desk			800-457-3642			
	Law Enforcement						
	Fire Department						
	Hospital						
	Ambulance						

Comment [I1p1]: Home Phone, Mobile Phone – Sensitive information? Should we label as such? –Sue Krieg



Emergency Contact
Information Template

FOR OFFICIAL USE ONLY
A-1

APPENDIX B LOCATION INFORMATION TEMPLATE AND INSTRUCTIONS

This appendix is designed to collect site specific information including location of backup tapes, building access, preventive controls, and the IT alternate site location.

Instructions for Completing the Location Information Template

OIP Site # - Enter the OIP Site # for this location.

Location Name - Enter the facility name, street address, and phone number.

Location IT Point of Contact - Enter the name, phone number, and email address of the IT point of contact (POC) for this location. Also, enter the Express Mail Account Number.

of CCE Workstations - Indicate the total number of workstations at the location that have the standard CCE Coreload.

of Non-CCE Workstations - Indicate the total number of non-CCE workstations at the location and give a brief description.

Backup Tapes

Locations 1, 2, 3 - If backup tapes are stored at more than one location, for each location, enter the building name, street address, phone number, and hours of operation of the building where the backup tapes are stored. For the location of the Safe Deposit Keys, if applicable, enter the building name, street address, phone number, contact name, and hours of operation.

Who Can Access - For each location, enter the name, phone number, and e-mail address of the person who can access the backup tapes. For the Safe Deposit Keys, enter the name, phone number, and e-mail address of the person who can access the keys.

Alternate IT Site - Enter the building name, street address, contact name, contact phone number, contact e-mail address, and directions to the alternate IT site location.

Note: Since OCIO-ITS can support Agency requirements remotely, you must select a site to restore IT Operations. This site can be selected independent of the Agency recovery efforts.

Preventive Controls - List the preventive controls for this location. Preventive controls can include: backup power supply, air conditioning, fire extinguisher, sprinkler system, off-site storage, security.

Note: Please use the Excel spreadsheet version of this template (see icon blow) to collect the information from each site.



State &
County_Location Ter

Location Information Template

OIP Site Number: _____

Location Name: _____

Street Address: _____

Phone: _____

Location IT Point of Contact (POC)

Name: _____

Phone: _____

E-mail: _____

Express Mail Account Number: _____

of CCE Workstations: _____

of Non-CCE Workstations:
(Include description) _____

Backup Tapes

Location 1:

Building Name: _____

Street Address: _____

Phone: _____

Hours: _____

Who Can Access:

Name: _____

Phone: _____

E-mail: _____

**Safe Deposit Keys Location
(if applicable)**

Building Name: _____

Street Address: _____

Phone: _____

Contact Name: _____

Hours: _____

**Safe Deposit Keys:
(who can access)**

Name: _____

Phone: _____

E-mail: _____

Backup Tapes

Location 2:

Building Name: _____
Street Address: _____

Phone: _____
Hours: _____

**Safe Deposit Keys Location
(if applicable)**

Building Name: _____
Street Address: _____

Phone: _____
Contact Name: _____
Hours: _____

Who Can Access:

Name: _____
Phone: _____
E-mail: _____

**Safe Deposit Keys:
(who can access)**

Name: _____
Phone: _____
E-mail: _____

Backup Tapes

Location 3:

Building Name: _____
Street Address: _____

Phone: _____
Hours: _____

**Safe Deposit Keys Location
(if applicable):**

Building Name: _____
Street Address: _____

Phone: _____
Contact Name: _____
Hours: _____

Who Can Access:

Name: _____
Phone: _____
E-mail: _____

**Safe Deposit Keys
(who can access)**

Name: _____
Phone: _____
E-mail: _____

Alternate IT Site

Building Name: _____

Contact Name: _____

Street Address: _____

Phone: _____

E-mail: _____

Directions to the Site: _____

Note: Since OCIO-ITS can support agency requirements remotely, you must select a site in which to restore IT Operations. This site can be selected independent of the Agency recovery efforts.

Preventive Controls

List Preventive Controls for this

Location: _____

(Examples include: backup power supply, air conditioning, fire extinguisher, sprinkler system, off site storage, security.)

FOR OFFICIAL USE ONLY

B-2

APPENDIX C IT DAMAGE ASSESSMENT FORM AND INSTRUCTIONS

Description on how to use this form:

This form should be filled out immediately upon recognizing a potential disaster. The damage should be logged into this form then sent or communicated to the IT Group Manager. Fill in as much detail and specifics as possible in the detailed additional information section. If the question is not applicable to the type of damage then specify N/A.

Conduct an on-site inspection to determine what operations have been affected and which strategies will be implemented. The IT Group Manager will evaluate strategies to respond to the incident. The specific strategies and actions selected to address the particular situation become the Recovery Recommendations.

NOTE: ACCESS TO THE FACILITY FOLLOWING A FIRE OR POTENTIAL CHEMICAL CONTAMINATION WILL LIKELY BE DENIED FOR 24 HOURS OR LONGER.

Building access permitting, conduct an on-site inspection of all affected areas to assess damage to the following:

- Electronic equipment (destruction, short-term restoration, and immediate suitability of use -- not long-term salvage potential).
- IT Vital records -- hard copy (files, manuals, documentation, etc.) and data on other media (personal computer data) -- to assist in finalizing actual IT recovery strategies and determining an overall restoration/salvage plan.
- Electronic equipment and telecommunications repair time (CCE Infrastructure, Workstations/Non-CCE Infrastructure Workstations, telecommunications equipment).
- Physical facility (environmental conditions, physical structure integrity).

Following the on-site inspection, instruct team members to report to the Alternate Site to participate in an assessment review meeting. Review the following information during this meeting:

- Documented assessment results using the IT Damage Assessment Form
- Salvage priorities on the above, noting which IT vital records and electronic equipment are needed for recovery activities and could be operationally restored and retrieved quickly, or those, which have the greatest potential adverse effect on the company.

NOTE: USDA guidelines for Proper Disposal of hardware/software **MUST** be followed.

IT Damage Assessment Form

OIP Site ID #:

Site Location/ City, State:

Contact Information:

No.	Description	Assessment							
		Physical Damage		Cabling Damage		Operational		Estimated Repair	
		Yes	No	Yes	No	Yes	No	Date	Time
1	Building/Facility							/	:
2	Electric/Power Service							/	:
3	Phone Service- Local LAN Line (PBX Switch)							/	:
4	LAN/CCE Infrastructure Physical Security of Infrastructure Network Connectivity Servers Workstations Cabinets/Racks							/	:
5	AS/400 System							/	:
6	SUN System							/	:
7	Printing Capabilities							/	:
8	Tape Availability	Yes	No					/	:
9	IT Vital Records	Yes	No					/	:
Logical Assessment (Sign on Capability)									
10	System Access							/	:
	Client/Server	Yes	No					/	:
	AS/400	Yes	No					/	:
	Sun	Yes	No					/	:

No.	Detailed Assessment Information
	<i>Provide as much detailed information as possible</i>
Physical Assessment	
1	Building/Facility Damage:
2	Electric/Power Damage:
3	Phone Service Damage:

Detailed Assessment Information <i>Provide as much detailed information as possible</i>	
4	<u>LAN/CCE Infrastructure Damage</u> (Include quantity available if applicable) Network Connectivity: Servers: CCE Workstations: Non – CCE Workstations: Cabinets/Racks:
5	AS/400 Hardware Equipment Damage:
6	SUN System Damage:
7	Printing Capabilities Damage:
8	Tape Availability Damage:
9	IT Vital Records Damage:
Logical Assessment	
10	System Access (Sign on capability) <i>If answered No on page 1, describe in detail why the system is not accessible and what it will take to get the system to a Sign on capability.</i>

Signature: _____ Date: ____ / ____ / ____

APPENDIX D SHORT AND LONG TERM SYSTEM REQUIREMENTS

This appendix identifies the short and long term recovery and reconstitution requirements for State Offices, Service Centers, and SCA Partner Specialty Offices. The appendix includes a list of hardware and software required to establish contingency operations and restore long-term operations.

TABLE D-1 SHORT TERM SYSTEM RECOVERY REQUIREMENTS

SYSTEM COMPONENT/ SERVICE	COMPONENT/SERVICE DESCRIPTION	QTY	VENDOR INFORMATION
CPUs	Gateway E4100	Varies by site	
Monitors	17" View Sonic	"	
Laptops	Gateway E450 Laptop	"	
Printer – Black & White	HP4200	"	
Printer – Color	HP4600	"	
Printer – WFC	HP2600	"	
Printer – Portable	HP350	"	
Printer – AS/400	4224 printer	"	
Fax Machine	Danka L621 with toner and drum	"	
Switches/Routers/Hubs		"	
AS/400 Console	3180 Workstation Console (AS/400)	"	
AS/400 Server & O/S		"	
Telephone handsets	8 button telephone handset	"	
Telephone handsets	16 button telephone handset	"	
Patch Panel/Cabling/Cabinet		"	
Disk Array (External)		"	
Fiber Optic Links		"	
Data Circuit		"	
Common Applications		"	
Supplemental Apps by Agency		"	
Cell Phones		"	
CCE Coreload			

* Critical for a State Office

TABLE D-2 LONG TERM SYSTEM RECONSTITUTION REQUIREMENTS

SYSTEM COMPONENT/ SERVICE	COMPONENT/SERVICE DESCRIPTION	QTY	VENDOR INFORMATION
UPS		Varies by Site	
Copiers		“	
PDA/Tablets		“	
GIS		“	
USB		“	
Scanners (Large)		“	
Scanner (State Office- RD)	Fujitsu Model 4097D (including Dell PC and flat panel monitor)	“	
SUN (OS/Apps)		“	
SQL/Oracle		“	
Plotters		“	
Print Shops		“	
Picture Tel		“	
Digital Cameras		“	
Tape Library (State Office)			

APPENDIX E RECOVERY DOCUMENTS LIST

This appendix provides a listing of recovery documents for the OCIO-ITS recovery teams to follow to ensure that all necessary recovery procedures are completed in the proper sequence. Copies of these documents can be found at the CCE Team Services web site which can be accessed at the following URL <http://century.its.nrcs.usda.gov/cce-states/>. A user name and password are required to access this web site.

State & County ITS Recovery Documents List

No.	Document Name	Document Type	Web Site Quick Launch Heading
1	02-IRM_R03_A01	Adobe Acrobat Document	Disaster Recovery
2	2001 CCE Workstation Installation Guide_Dell Mid-range_High-End	Adobe Acrobat Document	Workstation & Printer Guides
3	2001CCE_PrinterInstallationGuide	Adobe Acrobat Document	Workstation & Printer Guides
4	2002_CCE_Printer_Installation_Guide_final	Adobe Acrobat Document	Workstation & Printer Guides
5	2002_Compag_Proliant_ML370_Server_Setup_Guide_2.0	Adobe Acrobat Document	CCE Server Guides
6	2002_ProLiant_ML370_Server_System_Administration_Guide-Final_Ver.4	Adobe Acrobat Document	CCE Server Guides
7	2003 Windows_XP_Install_Guide_v3.0	Adobe Acrobat Document	Windows XP Migration
8	Acquisition Process for Replacement of CCE Equipment (01-10-2005)	MS Word Document	Disaster Recovery
9	Acquisition Process for Replacement of Infrastructure CCE Equipment (01-10-2005)	MS Word Document	Disaster Recovery
10	AD_File_Decompression_Guide_Ver2_0	Adobe Acrobat Document	CCE Server Guides
11	Add_Proced_Join_WKS_Usr_Domain_For_Exchge	Adobe Acrobat Document	CCE Server Guides
12	APC_Configuration_Guide_Final	Adobe Acrobat Document	CCE Server Guides
13	ArcGIS8.3DesktopSP3	zipped file	Supplemental Applications and Instructions
14	ArcGIS8.3DesktopSP3InstallGuide	Adobe Acrobat Document	Supplemental Applications and Instructions
15	arcgis-83-instructions	Adobe Acrobat Document	Supplemental Applications and Instructions
16	ARTS User Manual	Adobe Acrobat Document	Supplemental Applications and Instructions
17	AS400 Recovery Procedures Checklist (07-15-2004)	MS Word Document	Disaster Recovery
18	auto tape loader install inst	Adobe Acrobat Document	CCE Server Guides
19	Backpack_External_CDROM_Installation_Guide_v1.0	Adobe Acrobat Document	Workstation & Printer Guides
20	Brio Explorer 6.6.3.15 Update Installation Guide	Adobe Acrobat Document	Supplemental Applications and Instructions
21	CCE Serv Sec Pol-Chpt 1 FINAL DRAFT-subj-to-approv 022803	MS Word Document	Security
22	CCE Serv Sec Pol-Chpt 2 FINAL DRAFT-subj-to-approv 063003	MS Word Document	Security
23	CCE_OpenRackInstallationPhotos	Adobe Acrobat Document	CCE Server Guides
24	CCE_Server_System_Administration_Guide_Appendix_Q_MSWord_Format	MS Word Document	CCE Server Guides
25	CCE_Server_Update_CD1_Admin_Guide	Adobe Acrobat Document	CCE Server Guides
26	ClientAccessPostXP	Adobe Acrobat Document	Supplemental Applications and Instructions
27	Common Agency CD 3-6 Install GuideU2	Adobe Acrobat Document	Supplemental Applications and Instructions

FOR OFFICIAL USE ONLY

28	Common Agency CD 3-6 Install GuideU3	Adobe Acrobat Document	Supplemental Applications and Instructions
29	Common Agency Applications Guide v1	Adobe Acrobat Document	Supplemental Applications and Instructions
30	Config_Procedures_Domain_User_Accts_Ver_1	Adobe Acrobat Document	CCE Server Guides
31	CSToolkit2004V5.0_IG_v1_9	Adobe Acrobat Document	Supplemental Applications and Instructions
32	Data Circuit Recovery Checklist (09-16-2004)	MS Word Document	Disaster Recovery
33	DNR Garmin 4.4.2 Installation Guide	Adobe Acrobat Document	Supplemental Applications and Instructions
34	E4100 OpenGL Video Driver Update Support ArcMap App	Adobe Acrobat Document	Supplemental Applications and Instructions
35	Email Troubleshooting Guide -rev4.6	Adobe Acrobat Document	Exchange
36	Extending_DHCP_Range	Adobe Acrobat Document	CCE Server Guides
37	FSA PC18 DALRS Install	Adobe Acrobat Document	Supplemental Applications and Instructions
38	FSA-PostXPCottonInstall	Adobe Acrobat Document	Supplemental Applications and Instructions
39	Geodata Management Utiliy Guide	Adobe Acrobat Document	GIS
40	helpdesk escalation procedure v1.3	Adobe Acrobat Document	Exchange
41	HP4200 Printer Installation Guide_signed	Adobe Acrobat Document	Workstation & Printer Guides
42	Installation Instructions for NRCS Applications	Adobe Acrobat Document	Supplemental Applications and Instructions
43	Managing Geospatial Datasets Manual ver. 4.0	Adobe Acrobat Document	GIS
44	MapSource5.4InstallationGuide	Adobe Acrobat Document	Supplemental Applications and Instructions
45	McAfee Reinstall	Adobe Acrobat Document	Supplemental Applications and Instructions
46	Misc Hardware - RD Procurement Process (11-30-2004)	MS Word Document	Disaster Recovery
47	NFC_Entrust_Installation	Adobe Acrobat Document	Supplemental Applications and Instructions
48	NRCS_Brio66install	Adobe Acrobat Document	Supplemental Applications and Instructions
49	Olympus C-4000 Digital Camera Installation Guide_signed	Adobe Acrobat Document	Workstations & Printer Guides
50	OmniForm	Adobe Acrobat Document	Supplemental Applications and Instructions
51	Powering Down the AS400 (07-27-2004)	MS Word Document	Disaster Recovery
52	Powering down UPS & Compaq Servers (06-15-2005)	MS Word Document	Disaster Recovery
53	RD_BRIO_Install_revised	Adobe Acrobat Document	Supplemental Applications and Instructions
54	RD_Supplemental_Applications_CD_Guide_v1	Adobe Acrobat Document	Supplemental Applications and Instructions
55	Reconfig ODBC Connections	Adobe Acrobat Document	Supplemental Applications and Instructions
56	reloadModel170rev2(AS400)	MS Word Document	Disaster Recovery
57	SIR Handbook 2005 Install Instructions	Adobe Acrobat Document	Supplemental Applications and Instructions
58	slip-d	HTML	Disaster Recovery
59	SLIP-V Document (Version 2.5; 12-22-2000)	MS Word Document	Disaster Recovery
60	SpeedyCDInstallationGuidep	Adobe Acrobat Document	Supplemental Applications and Instructions
61	state IT Support Processes v1.2	Adobe Acrobat Document	Exchange
62	State_IT_Exchange_Guide_finalv3	Adobe Acrobat Document	Exchange
63	StorageWorks_External_Array_Config_Guide	Adobe Acrobat Document	CCE Server Guides
64	Telecom Checklist (10-28-2004)	MS Word Document	Disaster Recovery
65	Telecom EMERGENCY SUPPORT SUMMARY 1(09152004)	MS Word Document	Disaster Recovery

FOR OFFICIAL USE ONLY

66	Veritas System Administration Guide	Adobe Acrobat Document	CCE Server Guides
67	Voice-FAX Recovery Checklist (09-16-2004)	MS Word Document	Disaster Recovery
68	XP - FSA_Netscape_Brio_Plugin	Adobe Acrobat Document	Supplemental Applications and Instructions
69	XP_admin_guide_v2	zipped file	Windows XP Migration
70	XP_Ref_Guide_v3	Adobe Acrobat Document	Windows XP Migration
71	XServer 9.4 Install Instructions	Adobe Acrobat Document	Supplemental Applications and Instructions

APPENDIX F DAILY OPERATIONS LOG

Agency Name: _____

System Name: _____ Location: _____

Date: _____ Time: _____

Reporting Period Covered: _____

Operations Log Prepared By: _____

Emergency Activities Performed Since the Last Reporting Period in Sequential Order:

System Status: _____ Fully Operational
 _____ Partially Operational
 _____ Unavailable
 _____ Not Applicable

Reconstitution Status: _____ Original/New Site Fully Operational
 _____ Original/New Partially Operational
 _____ Original/New Unavailable
 _____ Not Applicable

Key Activities Since Last Report: _____

Personnel Status: _____

Other Comments: _____

