Information Technology Disaster Recovery Plan (ITDRP) Guidelines and Checklist

Agency Guidelines

Agency for Enterprise Information Technology
Office of Information Security

August 2007

I. PURPOSE

This guidance document provides instructions, recommendations, and considerations for the Executive Branch of the State of Florida government to use when developing their Information Technology Disaster Recovery Plan (ITDRP). ITDRP includes the interim measures to recover information technology services following an emergency or system disruption; however it starts with the mitigation measures to assure the continual performance of the IT systems, networks and integrity of data. This document defines the essential elements that should be included in a disaster recovery plan to assure the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

II. APPLICABILITY

This guidance is applicable to all IT organizational elements of the State of Florida including, but not limited to:

A) Executive Branch agencies,
B) Vendors and third party organizations providing IT products, services and/or support.

III. DISTRIBUTION

This guidance document shall be distributed to the Heads of the State of Florida agencies, Chief Information Officers, designated Emergency Coordination Officers/State Agency Continuity of Operations (COOP) Coordinators, IT Disaster Recovery Planners, and other interested parties.

IV. AUTHORITIES

A) Section 282.102, Florida Statutes (Communications and Data Processing)
B) Section 281.301, Florida Statutes (Security systems; records and meetings exempt from public access or disclosure)

V. REFERENCES

A) Section 252.365, Florida Statutes (Emergency coordination officers; disaster-preparedness plans)
B) Continuity of Operations Implementation Guidance, Division of Emergency Management, Department of Community Affairs, September 9, 2002
C) Executive Memorandum (Computer Security Incident Response Team (CSIRT) Training), February 3, 2003
D) Executive Memorandum (Agency IT Disaster Recovery Plan, joint issue by the State Technology Office and Division of Emergency Management, May 13, 2003

VI. BACKGROUND

As part of each agency's Continuity of Operations (COOP) plan there is a requirement to assure that each agency's Disaster Recovery Plans are capable of supporting COOP activities in accordance with Florida Statutes, Chapter 282, Communications and Data Processing. One of the Essential Elements of the COOP Implementation Guidance is that each agency's COOP plan includes elements that cover Vital Records and Databases. The element of Vital Records and Databases is defined in the Division of Emergency Management to me an, "Each agency should provide for the protection and availability of electronic and hardcopy (as applicable) of documents, references, records, information systems, and databases."

This guide has been developed to provide the general guidelines for building Information Technology Disaster Recovery Plans (ITDRP) and to help agencies understand the key elements that should be considered to assure IT operations are fully covered in their Disaster Recovery Plans.

VII. GENERAL GUIDANCE

In planning for disaster recovery, each agency must identify potential threats to its information technology needs. Based on those assumptions, each agency must analyze what needs to be achieved in order to carry on as though the disaster never happened.

A) Plan for how to address the smallest incident all the way to a major disaster.
B) Assure the ongoing viability of the ITDRP, once implemented it must be tested and exercised and revised as necessary.
C) Include a well-defined data backup and recovery plan within the ITDRP.
D) Remember the integrity and availability of data are essential to a successful recovery of critical business functions.
E) Adhere to standardized, purposes, objectives and definitions of terms. A standard set of definitions is included later in this guide.
F) Include detail how systems can be restored in different scenarios and describe how systems can be rebuilt to resume normal operations.
G) Plan to have a recent and reliable copy of all the data.
H) Keep your backups located far enough away from your primary IT operations to reduce the likelihood they are impacted by the same disaster.
I) Plan for the IT operations needed to recover the "end user" and the network communications required between the IT organization and the end user recovery site.
J) Begin planning for disasters early in the development project life cycle for new systems and introduction of new technology.

VIII. OBJECTIVE

The agency's ITDRP must cover the critical operations, processes and applications along with their dependencies with other critical elements. Due to increasing dependencies on information technology for mission essential functions, it is important to understand the true scope of what a disaster recovery program entails. In today's complex IT designs, applications and processes become dependent on diverse systems to operate. If a significant business interruption occurs, the ability to restore a critical business process may depend on a host of systems that may not even be located at the same site.

This ITDRP guide will help the agency develop a comprehensive disaster recovery plan. The ITDRP guide is not intended to present the only way to develop an ITDRP. Each organization is responsible for selecting their own methodology for completing their plan. The guides and suggestions in this document are just that: guides and suggestions. Use the information in the guide as the minimum starting point in developing an ITDRP specific to the agencies structure and needs.

Note: It is not the intent of this guide to have the agency re-write its ITDRP. If an agency has developed an ITDRP using another format or methodology there is no need to reformat it to conform to this guide.

IX. ESSENTIAL ELEMENTS OF ITDRP

This guide is designed around the planning elements found in the "Best Practices" for IT Disaster Recovery Plans. Once these elements are understood, it will become clear that ITDRP is an ongoing process and not a one-time event, and, like the COOP plans, the ITDRP elements are the essential areas for planning for a full range of potential emergencies.

- **Element 1.** Purpose
- **Element 2.** Asset Management
- **Element 3.** Application Analysis
- **Element 4.** Business Impact Analysis
- **Element 5.** Risk Analysis
- **Element 6.** Emergency and Incident Response
- **Element 7.** DRP/Data Storage Strategy
- **Element 8.** Recovery Plan
- **Element 9.** End User Recovery
- **Element 10.** Networking Backup
- **Element 11.** Maintenance, Exercise and Testing
- **Element 12.** Change Management

Each agency may be in different stages of planning, whether they are just beginning to plan or already have a comprehensive data center recovery plan. Regardless of which stage an agency is in, ensuring that all 12 key elements are integrated into its disaster recovery program is an important step in the creation and maintenance of an effective ITDRP.

The remaining sections of this guide address the Essential Elements of an effective Information Technology Disaster Recovery Plan.

Element 1. *Purpose*

The first element of IT disaster recovery planning is usually self-evident to IT professionals. As a profession they know their task is to keep the information systems operating so the business can continue to serve its citizens/customers. Keeping systems secure and planning to restore data in cases of interruptions are normal processes for most IT departments.

In today's environment where the agencies are beginning to develop COOP plans, the IT departments have an opportunity to reassess the reasons why they have an ITDRP and check the scope, objectives and assumptions of the plan to assure the plan covers what is important to the business. In most cases the plan should be based on information that was developed in the business section of the COOP and business impact analysis plan.

Planning for this element includes:

1.1 Definitions (Refer to the standard set included in Section XI)

1.2 Strategy and Policy - Every IT organization needs an IT disaster recovery policy. Whether a disaster recovery policy is currently in place or one needs to be created, the IT organization should consider several things. First, the plan should reflect the objectives of the COOP program. The creator of the policy must understand the expectations and limitations of the organization and its leadership. The same considerations should be taken when defining the disaster recovery strategy. The strategies should drive the policy, and the policy, if endorsed and enforced will be effective and will serve as a guide to the program overall.

1.3 Regulatory Requirements - To define the disaster recovery requirements of an organization, mandates set by regulatory agencies must be documented and understood. Although regulatory organizations for many agencies require disaster recovery plans, little guidance is provided on how to accomplish this goal. The responsibility falls on the agency to establish a strategy to achieve regulatory compliance.

1.4 Scope - The scope and limitations provide focus for the planning effort. The plan's scope should encompass all critical IT functions. The plan must be based on "Worst Case Scenario", which would include the inaccessibility or unavailability of the agency's IT facility or building complex and all its contents. Consider any identified hazards or peaks discovered in the Agency's COOP. Based on the analysis of this information, the plan may have more than one scope and several limitations.

1.5 Assumptions - The plan being created should be built on some basic assumptions. This narrows the possibilities --instead of writing one plan for fire, one plan for flood, one plan for explosion, there will be one plan written to cover an interruption that would affect operations for 30 days or more, regardless of what type of incident. Under the assumed circumstances, the plan would take effect.

If something outside the realm of those assumptions occurs, the plan base could be used and alternatives would have to be considered. You may have more than one plan assumption, based on the peaks identified through a business impact analysis.

Element 2. *Asset Management*

When establishing an IT disaster recovery plan, it is essential to maintain an accurate database of information technology assets. Just as an agency must understand the mission essential elements of its business the IT organization must know what assets support those business elements. It is extreme ly difficult to know what to recover if an organization does not know what assets exist. Not only is this information needed for planning response and recovery but also it is vitally important to have this information for restoration following a major loss of building and/or equipment.

Information needed for planning this element includes:

2.1 Hardware with serial numbers.
2.2 Software with license numbers.
2.3 Vendor information.
2.4 Network schematic diagrams.
2.5 Setup and configuration information.
2.6 Equipment room floor grid diagrams.
2.7 Contract, maintenance and replacement agreements.
2.8 Special operating instructions for sensitive equipment.
2.9 Cellular telephone inventory and agreement.

Element 3. *Application Analysis*

Not only must the agency maintain a list of its IT assets, it must also include a comprehensive inventory of its applications. It is imperative they include the interdependencies of the application with other applications and other systems. With the complexity of web-based applications, these interdependencies may be with systems and applications not even under the responsibility of its IT organization.

Information gathered for this analysis includes:

3.1 Component name and technical identification.
3.2 Type (online, batch process, script).
3.3 Frequency.
3.4 Run time.
3.5 Allowable delay (days, hours, minutes, etc.).
3.6 Business Owner.
3.7 System dependencies.

Element 4. *Business Impact Analysis*

The IT disaster recovery planning team needs to identify which agency departments, functions, or systems are most vulnerable to potential threats and what, each identified potential threat may have on each vulnerable area within the agency. Without input from agency management, recovery priorities, recovery time objectives (RTOs) and other such recovery requirements are likely to reflect IT's perspective and may not necessarily reflect actual agency needs.

An information technology only recovery plan without a corresponding COOP plan, only addresses part of the disaster recovery solution. Having an IT disaster recovery solution without an agency COOP plan could result in planning for expensive recovery sites for the wrong computer applications; that don't support the most important mission essential functions of the agency.

The disaster recovery planning team should work closely with the COOP planners to identify which agency departments, functions, or systems are most vulnerable to potential threats. Planning for this element includes:

4.1 Identify functions, processes, and systems.
4.2 Interview information systems support personnel. Interview business unit personnel.
4.3 Analyze results to determine critical systems, applications, and business processes.
4.4 Prepare impact analysis on interruption on critical systems.

Element 5. *Risk Analysis*

Understanding the risks an agency faces is important to planning measures to mitigate them. Using the regulatory requirements discussed in Element 1 as a guide, and capitalizing on the knowledge of subject matter experts in IT security and risk analysis, agencies can assess the gaps in current practices and identify exposures to risks that can impede its IT operations.

A complete risk assessment includes both external risks and internal risks. External risks include environmental hazards and natural disasters. Internal risks include poor business practices that could result in unnecessary interruptions or ineffective responses to various events. If necessary, the scope of an assessment can be narrowed down to IT business practices alone.

The IT disaster recovery planning team needs to work with the agency's technical and security person and determine the probability of each mission essential function and corresponding system(s) becoming severely disrupted. They should then document the amount of acceptable risk the agency can tolerate.

Planning for each critical system should include:

5.1 Review physical security, (i.e. secure office, building access off hours, etc.).
5.2 Review backup systems and data security.
5.3 Review policies on personnel termination and transfer.

5.4 Identify systems supporting mission-critical functions.
5.5 Identify vulnerabilities, such as physical attacks, or acts of God, such as floods.
5.6 Assess probability of system failure or disruption.
5.7 Review provisions for ensuring cyber security of data and networks.
5.8 Prepare risk and security analysis.

Element 6. *Emergency and Incident Response*

Emergency response procedures must be defined, once the direction of the program, risks to the organization and the priorities are established. As the lifecycle of the program continues the procedures will be modified and enhanced. However, even in the beginning, it should be understood by those responsible for disaster recovery, what is expected of them to manage the response to an event.

Components of the emergency response plan include:

6.1 An effective emergency response team within the IT organization.
6.2 A process in place to provide decisions and direction to all the teams that are responding to a disaster.
6.3 A provision to include the Computer Security Information Response Teams (CSIRT).
6.4 Training to IT staff and a walkthrough of the IT components of the COOP emergency management process to ensure that it is current and that all members understand the plan strategies and know their roles.

Element 7. DRP/Data Storage Strategy

Normal operating procedures for the IT department should be checked to assure that nightly backups of data are routinely being done and that backups are being sent off-site. As part of this element, backup schedules and off-site rotations need to be checked for alignment with data recovery requirements. Data gathered from performing the application analysis and business impact analysis will establish these requirements as well as priorities for disaster recovery planning. Once it is understood what applications exist, their interdependencies and the criticality of those applications, solutions can be established to manage the critical systems and their data.

This process cannot happen without considerations for data availability. Application criticality will coincide with data criticality in a general sense. A team of IT disaster recovery and data management staff working together, can develop a joint systems and data classification scheme to meet recovery objectives. Normally the IT department would look to the business impact analysis for the recovery objectives; if a business impact analysis hasn’t been conducted then the IT department will need to meet with agency management to check the Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to classify applications.

Information gathered in this element must identify all vital records and data including:

7.1 Name and description.
7.2 Type (backup, original, master, history).
7.3 Where the vital records and data are stored.
7.4 Source of data, item, or record.
7.5 Alternate sources (if available where the data or record can be easily replaced by another source).
7.6 Backup and backup generation frequency.
7.7 Number of backup generations available onsite and off-site.
7.8 Location of backups.
7.9 Media key, retention period, rotation cycle.
7.10 Who is authorized to retrieve the backups.

Element 8. *Recovery Plan*

This element involves the development of an actual document that defines the resources, actions, tasks and data required to manage the recovery of the IT operations in the event of an interruption. This document becomes the plan used to assist in restoring the IT data and processes within the stated recovery goals. The IT disaster recovery coordinator would have this document available to them in an emergency, and should use it along with the assistance of the IT disaster planner.

A comprehensive ITDRP should include:

8.1 Objective --This should be a summation of all the requirements developed in the earlier elements and should fully support the objectives set forth in the agency COOP plan.
8.2 Plan Assumption
8.3 Criteria for invoking the plan

1 Document reasons to activate the ITDRP that do not justify activation of the COOP.
2 Document an emergency response procedure to cover actions that occur during and after an emergency is declared for that agency. After the emergency, check the building before allowing individuals to enter.
3 Document procedures for assessment and for declaring a state of emergency.
4 Document notification procedures for alerting all senior management executives, disaster recovery team members, COOP coordinators and agency executives.
5 Document notification procedures for alerting IT personnel of alternate location.

8.4 Role Responsibilities and Authority

1 Identify IT disaster recovery team and agency functional personnel
2 IT Recovery team description and charge
3 IT Recovery team staffing
4 Vendor roles and responsibilities
5 Transportation schedules for media and teams

8.5 Procedures for operating in contingency mode

1 Process descriptions
2 Minimum processing requirements
3 Determine categories for vital records
4 Identify location of vital records
5 Identify forms requirements
6 Document critical forms
7 Establish equipment descriptions
8 Document equipment --in the recovery site and in the agency
9 Software descriptions
10 Software used in recovery and in production
11 Produce logical drawings of communication and data networks in the agency
12 Produce logical drawings of communication and data networks during recovery
13 Vendor list
14 Review vendor restrictions
15 Miscellaneous inventory
16 Communications needs --production and in the recovery site

8.6 Resource plan for operating in contingency mode
8.7 Criteria for returning to normal operating mode
8.8 Procedures for returning to normal operating mode
8.9 Testing and Training (Refer to Element 11. Maintenance, Exercise and Testing for more information about this section)

1 Document testing data
2 Complete disaster/disruption scenarios
3 Develop action plans for each scenario

8.10 Plan Maintenance (Refer to Element 11. Maintenance, Exercise and Testing for more information about this section)

1 Maintenance review schedule (yearly, quarterly, etc.)
2 Maintenance review action plans.
3 Maintenance review recovery teams.
4 Maintenance review team activities.
5 Maintenance review/revise tasks.
6 Maintenance review/revise documentation.

8.11 In addition, a communication plan should be outlined -- how the ITDRP teams will communicate with the COOP coordinator, vendors, the Command center, their management team, and how the employees will be notified, who will be notified, etc. This section should also outline where the “command center” will be set up and what will be needed at that site.
8.12 Reporting Structure -The reporting structure has the potential to be different than the IT structure during normal operations. Not all areas of normal operations will be activated

in the event of a prolonged outage. This element should include a graphical representation of the ITDRP teams' reporting structure.

Element 9. *End User Recovery*

In the past, traditional ITDRP focused rather narrowly on the recovery of the IT side of the agency functions; recovering technology platforms, mission essential applications, their data, their servers and the network infrastructure components. In today's world, end users must consider their own disaster recovery plans as part of their Continuity of Operation plans. While IT is recovering its IT operations, the end-users may simultaneously moving to alternate facilities to recover the business side of the agency operations.

The end users will need assistance with IT equipment and communications therefore the ITDRP should include activities for:

9.1 IT components needed at alternate end-user recovery sites such as telephones, local area networks, client side applications, and security.
9.2 Remote access capabilities.
9.3 Recovery at commercial recovery centers and mobile recovery centers and the connectivity back to the IT operations.
9.4 Redirection of voice telecommunications.

Element 10. Networking Backup

ITDRP is more than just planning for the backup and recovery of applications, data, and systems that support the agency's essential functions. Consideration has to be made for network recovery planning.

An agency has to formulate plans to cover three discrete areas of networks:

A) Internal agency networks (the networks that run the departmental or workgroup local area networks via a switched or routed backbone network).

B) SUNCOM networks that connect the agency to other agency networks and to the Myflorida.com network.

C) Alternate network locations that provide means to recover mission-critical internal network services and to reroute SUNCOM network services and telephony services to alternate end user and/or IT recovery. Planning for this element is best done with the IT local area subject matter experts and the SUNCOM services telephony and network planners.

Planning for the restoration of wide area voice and data networking links following agency or system relocation includes:

10.1 Restore end-user access to the SUNCOM network. This may be done through a Value Added Service Provider with direct line connection(s) or via dial up remote access technology provided to the end-user.

10.2 Connect the IT operations at the alternate site to the SUNCOM network.

10.3 Assure security and integrity in the new network.

Element 11. Maintaining, Exercise and Testing

Having completed the first recovery plan is only the beginning. An ongoing program must be designed to keep the plan tested and maintained. The plans now become living documents and include valuable information that is essential to the ongoing viability of the IT department.

The plan must be maintained and tested regularly. This information includes but isn't limited to emergency response procedures, response teams, contact information for staff, customers and vendors, critical agency functions and the strategy for their continuity or recovery, and technical requirements for supporting these functions with their respective recovery strategies. Staff, technical, and agency business functions will change, and so must the plan.

Testing Program - Each ITDRP should include exercises to test the people and processes of the plan. The goal of these exercises is not to test as a pass/fail; rather they should be designed to identify opportunities to continuously improve the plan.

Each exercise should have clearly defined objectives to measure each test.
Each objective obtained may still require refinement in terms of issues, which have to be resolved during the exercise. These refinements may include improvements such as updating a vendor's contact information or revising a back-up procedure to save time with an application recovery.

Managers, who sign off on the objectives prepared for the exercise, and the post exercise results, may be evaluated by their superiors on the preparedness of the team members and plan effectiveness. Therefore, managers should be encouraged to view each exercise as a vehicle for improving their individual plans.

The following types of exercises should be conducted sequentially for every ITDRP in the agency:

11.1 Emergency Response Exercise– The agency's emergency management coordinator generally organizes these types of plans. Don't be surprised when one of these plans includes activating part of a COOP plan along with the ITDRP.

11.2 Structured Walk-Through (Table Top Exercise) – During what is commonly called a Table Top Exercise, participants test the ITDRP and its standard operating procedures by informally "walking through" a hypothetical emergency causing an interruption to the business. The structured walkthrough allows management, planners and key staff with emergency and disaster recovery responsibilities to identify and resolve problems in the plan.

11.3 Tactical/Simulated (Single process or Functional Area) – This type of exercise is more extensive than a Table Top exercise in that it involves activities in other than a conference room atmosphere. It is also more likely to be done in conjunction with activating the COOP plan for a limited number of facilities, business processes or systems. These exercises usually include the activation of a command post and may extend to actually relocating but doing a full recovery at an alternate location.

11.4 Operational (Multiple Processes or Interrelated Functional Areas) – These exercises are more extensive and realistic than either the Table Top or the Tactical/Simulated exercises. Activities extend beyond a conference room or operations center, taking place in alternate locations and lasting over several days.

Element 12. *Change Management*

IT organizations learn that disaster recovery planning is just another IT process, not a project with an end date and final deliverable that must be managed. New agency applications come on line; systems are moved, upgraded, or decommissioned; key resources are reassigned to new areas.
Most IT professionals have learned to use structured development techniques to manage other IT processes such as application development and system architectural design. A key strategy for incorporating DRP into the IT organization includes integration into the project lifecycle that the IT department uses for its other systems development processes. As new systems and applications come through the door, criticality and recovery requirements can be defined. In the project lifecycle, business availability objectives are defined in the initial stages. That is the best time to establish the technological solutions to meet these objectives.

Change management can be a powerful project lifecycle function for ITDRP. It supports both asset management and disaster recovery. From an asset management perspective, it keeps the data accurate and current. For example, when a server is being decommissioned and a change notice is issued, the change also occurs in the asset management database, assuming there is an automated feed from one database to the other. Otherwise the change must be done manually to maintain accuracy. The accuracy is critical from a disaster recovery perspective as the asset management database serves as the source for what needs to be recovered. Also, change management can reflect workflow. If a server needs to be brought down for an upgrade, the change notice should reflect which applications would be affected. This is important information for those using the applications, particularly in a 24/7 organization. This information is also very important to the disaster recovery planning process.

X. CONFIDENTIAL INFORMATION

Information concerning an Agency’s IT Disaster Plan is considered to be part of the agency’s security systems and therefore should be classified as confidential and marked accordingly.

Each completed ITDRP should be marked with a clear reference to the following Florida Statute.

281.301 Security systems; records and meetings exempt from public access or disclosure. -- Information relating to the security systems for any property owned by or leased to the state or any of its political subdivisions, and information relating to the security systems for any privately owned or leased property which is in the possession of any agency as defined in s. 19.011(2), including all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to or revealing such systems or information, and all meetings relating directly to or that would reveal such systems or information are confidential and exempt from ss. 119.07 (1) and 286.011 and other laws and rules requiring public access or disclosure.

XI. DEFINITIONS

A) Applications: Application software is system or network-level routines and programs designed by (and for) system users and customers. It supports specific business-oriented processes, jobs, or functions. It can be general in nature or specifically tailored to a single or limited number of functions.

B) Coldsite: A "Coldsite" is an empty computer room(s), ready to receive and support a replacement computer equipment configuration, equivalent to that defined to be recovered at an alternate site. The Coldsite may consist of a raised floor area equipped with: air conditioning, chilled water, power (60 Hz and 400 Hz), automatic fire detection and suppression systems, adequate security access control, and pre-positioned communications facilities. This room will be used to house equipment following activation of the Hotsite if an extended disaster situation is foreseen.

C) Continuity of Operations (COOP): Continuity of Operations is an effort within individual departments and agencies to ensure the continued performance of minimum essential functions during a wide range of potential emergencies. This is accomplished through the development of plans, comprehensive procedures, and provisions for alternate facilities, personnel, resources, interoperable communications, and vital records/ databases.

D) Computer Security Incident Response Teams (CSIRT): Computer Security Incident Response Teams are teams of key individuals within each State Agency trained to respond to computer security incidents internally. CSIRT is internally coordinated through OIS to respond, evaluate, correct and mitigate Cyber incidents within agencies.

E) Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

F) Disaster: An event that creates an inability on an organization’s part to provide critical business functions for some predetermined period of time.

G) Disaster Recovery: The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization’s critical business functions.

H) Disaster Recovery Plan: The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster.

I) Hotsite: A "Hotsite" is a primary fully operational data processing facility, containing computer equipment that has been installed with a configuration that meets the agency's specifications as outlined in the requirements for recovery at an alternate site. This computer equipment configuration must be immediately available for use by the agency in the event of a disaster. It must contain all installed computer hardware, peripherals, telecommunications equipment, power, air conditioning, etc., to support the agency's specified hardware configuration.

J) Information Technology (IT): Information Technology and Services within the Departments.

K) Information Technology Disaster Recovery Plan (ITDRP): stands for the portion of the agencies Communications and Data Processing plans that covers the resumption and recovery of the Information Technology functions of the department or agency.

L) Networks: A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices that are used to transport information between systems.

M) Prevention Phase: This is generally defined as the first phase by many business continuity programs and refers to the positioning and implementation of those measures and activities that will lessen the impact of adverse incidents occurring in an agency. This document does not cover this phase.

N) Recovery Time Objective (RTO): A principal concept in contingency planning, for the purposes of this document, refers to the amount of time an organization could do without an IT-based business process.

O) Recovery Phase: The recovery phase of the ITDRP is the process of planning for and/or implementing expanded recovery operations of less time-sensitive operations after the most time-sensitive operations and functions have been resumed. This may be at the primary site or alternate site(s).

P) Recovery Point Objective (RPO): Another metric for disaster planning used to determine the point position of recovered data following any disaster event.

Q) Response Phase: This is generally the second phase described in business continuity methodologies. Processes covered in the phase are generally included in the agency’s Emergency Response Plans that covers the process of planning for and/or implementing the agency’s reaction to an incident or an Emergency. This phase may be initiated by the COOP coordinator as part of the activation of the agency COOP plan, however it is more than likely will be activated within the IT organization to respond to incidents within the IT organization that don’t justify activating the COOP plan. Procedures for responding to computer related incidents aren’t covered in this document and should be covered in the agency’s CIRT policy and procedures.

R) Restoration Phase: In regards to the ITDRP this phase involves the processes of the continuity plan to restore the contents with the IT processors and equipment or replacing the damaged or destroyed structure of the IT operations. This phase of the continuity plan starts after the damage assessment is done and continues until the IT operations are moved back from its resumption and recovery locations and IT operations are restored back to normal.

S) Resumption Phase: This is phase where the ITDRP starts and includes the process of planning for and/or implementing the resumption of only the most time-sensitive operations immediately following an interruption or disaster. This may involve activating a move to an alternate site.

T) Systems: A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data that is used in a production or support environment to sustain specific applications and business organizations in their performance of tasks and business processes.

U) System Software: The programs and routines used to employ and control the capabilities of the system, including, but not limited to, operating systems, utilities and library routines.

XII. ADDITIONAL REFERENCE MATERIALS

A. Disaster Recovery Planning: *Strategies for Protecting Critical Information Assets*, *2nd Edition, by Jon Toigo. 2000, 354 pages.*

B. Disaster Recovery Planning: Preparing for the Unthinkable, *3rd Edition, by Jon Toigo, 2002. 482 pages.*

C. Disaster Proofing Information Systems, *by Robert Buchanan. December2002, 288 pages.*

D. Primer for DRP in an IT Environment, *by Charlotte J. Hiatt. 2000, 276 pages.*

E. Security Planning & Disaster Recovery, *by Eric Maiwald, William-Sieglein. 2002, 299 pages.*

F. Manager's Guide to Contingency Planning: *Protecting Vital Facilities and Critical Operations, 2nd Edition, by Kenneth N. Myers. 1999, 256 pages.*

G. The Business Continuity Planning Guide, *by Strohl Systems, October 1995, 400 pages.*

APPENDIX A
Information Technology Disaster Recovery Plan (ITDRP) - Checklist

I. PURPOSE

This checklist is to be used when developing State Agency IT Disaster Recovery Plans (ITDRP). Each agency of the Executive Branch of the State of Florida should submit the IT Disaster Recovery portion of their Continuity of Operations (COOP) plan to the Office of Information Security (OIS). This should be done in parallel to the submission of their agency COOP plan to the Division of Emergency Management (DEM). Prior to submitting their ITDRP each agency shall complete this checklist as well and submit it along with their ITDRP.

The criteria for this checklist was prepared using the ***IT Disaster Recovery Planning Guidance*** dated June 2, 2003. The implementation guidance provides instructions to the Executive Branch of the State of Florida to develop and implement disaster recovery plans specifically for their IT organizations. These criteria will serve as the primary OIS review mechanism to ensure compliance for the State Agency's IT Disaster Recovery Plan.

These criteria are not intended to limit nor exclude additional documentation that the State Agency may decide to include to satisfy other relevant rules, requirements, or any special issues that the State Agencies deem appropriate or inclusion. Such voluntary inclusion will not be subject to the specific review by OIS, but only those items identified in the following criteria. Any additional information, which is included in the plan, will not be subject the specific review of OIS, although they may provide comments.

II. INSTRUCTIONS

NOTE: Sections A-F no longer apply to current documentation guidelines, historical placeholder reference to original 2003 document requirements only.

A) ***This form must be attached to the State Agency ITDRP portion of their COOP plan when submitted for review to the Office of Information Security. The agency's lead Information Technology executive must provide their signature on this document prior to submission to OIS. Their signature will serve as authorization that they have reviewed the State Agency IT Disaster Recovery Plan and assure that the ITDRP checklist was completed in accordance with the Purpose and Instructions. Additionally, the agency's COOP Coordinator shall provide their signature below to donate their review of the document.***

B) State Agencies should use this document as a cross reference to their ITDRP by listing the page number and paragraph where the criteria are located within their plan. A reply should be included in the appropriate cell for each item in the matrix. This will assure accurate and efficient coordination of the State Agency ITDRP plans with OIS.

NOTE: Section C no longer applies to current documentation guidelines, historical placeholder reference to original 2003 document requirements only.

C) The Agency COOP Coordinator should forward a copy of the document to OIS at the following address:

IT Disaster Recovery Coordination Checklists
Agency for Enterprise Information Technology
Office of Information Security
4030 Esplanade Way
Tallahassee, FL 32399-0950

D) Given the sensitive content in these documents copies should only be sent by certified mail or hand delivered.

E) The OIS ITDRP Coordinator shall review the checklist and ensure that it coordinates with the State Agency ITDRP plan by inserting an X mark for each element identified in the plan by the agency. The OIS ITDRP Coordinator shall note any resources that are over extended or tasked by multiple State Agencies, and report such over extensions to DEM for resolution.

F) Additionally, the Chief Information Security Officer/OIS COOP Coordinator shall provide their signature below to donate their review and completion of the document.

III. CONTACT INFORMATION

A. STATE AGENCY NAME

B. FACILITY(s) INFORMATION:

Include the following location information concerning the facilities where the Information Technologies of the agency operate.

Include in the list, locations for alternate site recovery for IT operations and location of backup data storage

Insert extra lines for additional locations.

Location	Name (s) or Description(s)	Location/Mailing Address (Street, City, State, Zip Codes)
1		
2		
3		
4		

Location	Duty Hours Emergency Contact		Non-Duty Hours	
	Contact Name	Number	Contact Name	Number
1 (reference to 1 above)				
2 (reference to 2 above)				
3 (reference to 3 above)				
4 (reference to 4 above)				

IV. ESSENTIAL ELEMENTS

Element 1. Purpose

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIS ITDRP Check (3)
Element (1.2)	IT Disaster Recovery Policies are in place which address the purpose, goals and objectives of the IT operations of the agency.		
Element (1.3)	Regulatory requirements that impact the agencies ITDRP have been identified and addressed in the plan.		

(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.

Element 2. Asset Management

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIS ITDRP Check (3)
Elements (2.1 to 2.9)	An accurate database (or file) system is maintained and referenced where information for IT asset is available for use in recovery and restoration.		

(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.

Element 3. Application Analysis

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIS ITDRP Check (3)
Elements (3.1to 3.6)	Comprehensive lists of agency applications have been included in the ITDRP that includes the timeframe when the applications should be recovered.		

Element (3.7)	System dependencies are identified for applications associated with mission critical functions.		
(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.			

Element 4. Business Impact Analysis

Cross Reference (1)	**Description**	**Page Paragraph Indicator (2)**	**OIS ITDRP Check (3)**
Element (4.1 to 4.4)	A Business Impact Analysis has been completed or the IT disaster planning team has met with the agency business owners to align the mission essential functions with the necessary IT applications and systems.		
(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.			

Element 5. Risk Analysis

Cross Reference (1)	**Description**	**Page Paragraph Indicator (2)**	**OIS ITDRP Check (3)**
Elements (5.1 to 5.6)	A risk assessment has been completed on internal and external risks to the IT department that includes data backup and protection practices and change management practices.		
Element (5.7)	Provisions for ensuring cyber security of data and networks have been incorporated into the planning process.		
(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.			

Element 6. Emergency Response

Cross Reference (1)	**Description**	**Page Paragraph Indicator (2)**	**OIS ITDRP Check (3)**

Elements (6.1 and 6.2)	Emergency organization for the IT operations and procedures are in place to provide for decisions and direction to all IT teams.		
Element (6.3)	Provisions to include the Computer Security Information Response Teams (CSIRT) are included in the plan.		
Element (6.4)	Training on emergency response procedures is included in the plan.		

(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.

Element 7. DRP/Data Storage Strategy

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIS ITDRP Check (3)
Element (7.1 to 7.6)	Normal operating procedures include routine backups of data with a clear strategy to identify all vital records and data.		
Element (7.7 to 7.10)	Backups strategy and procedures are in place to store and recover data off-site.		

(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.

Element 8. Recovery Plan
(*Note: this is the actual ITDRP document that should be submitted; not all sections of this element will be checked*)

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIs ITDRP Check (3)
Element (8.4)	Roles, responsibilities and authority are clearly defined in the plan.		
Element (8.5)	Procedures for operating in a contingency mode are included in the plan.		

Element (8.6)	Resource plans with recovery team structures for operating in a contingency mode are in the plan.		
Element (8.9)	Provisions for maintaining the plan are in place to keep the plan up to date.		
(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.			

Element 9. End User Recovery

Cross Reference (1)	**Description**	**Page Paragraph Indicator (2)**	**OIS ITDRP Check (3)**
Elements (9.1 and 9.2)	IT components required for the recovery of the end user are covered in the plan. (Components such as PCs, laptops, local servers for electronic lists of critical data, etc.)		
Element (9.4)	Redirection of telephone services are covered in the plan for the end user sites as well as the IT alternate operations sites.		
(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.			

Element 10. Networking Backup

Cross Reference (1)	**Description**	**Page Paragraph Indicator (2)**	**OIS ITDRP Check (3)**
Elements (10.1 and 10.2)	Network connectivity between the agency end user sites and the IT operations are included in the plan.		
Element (10.3)	Procedures are in place to assure the security and integrity are in place for temporary communications between alternate sites.		
(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.			

Element 11. Maintenance, Exercise and Testing

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIS ITDRP Check (3)
Elements (11.1 to 11.4)	A comprehensive testing program and testing procedures are in place to routinely exercise the plan.		

(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.

Element 12. Change Management

Cross Reference (1)	Description	Page Paragraph Indicator (2)	OIs ITDRP Check (3)
Elements (12.1)	Change management procedures are in place to keep the IT asset list or database updated when changes are made to systems or vital data for mission essential functions.		

(1) Cross Reference to ITDRP Guide; (2) To be Competed by Agency Planner prior to submittal indicating where this is addressed in the agency ITDRP; (3) To Be Completed by OIS after submittal.

Signatures and Authorizations

Approval Signature Block

Signatures and Authorizations (Completed Prior to Submittal to OIS)

Agency IT Executive/CIO signature	Date	(*Print Name*)
Agency ITDRP/COOP Coordinator signature	Date	(*Print Name*)

NOTE: This section no longer applies to current documentation guidelines, historical placeholder reference to original 2003 document requirements only.

Signatures and Authorizations (Completed After Review by OIS)

OIS ITDRP/COOP Coordinator signature	Date	(*Print Name*)
OIS Chief Information Security Officer signature	Date	(*Print Name*)