

Maricopa County Policies and Procedures	Subject: Disaster Recovery	Number: A1602 Issue Date: 1-02
Approved: <i>David Smith</i>	Initiating Department: Office of the CIO	

A. Purpose

County business operations and processes depend on a variety of resources to meet our customer's expected end-results. The introduction of technology has afforded Government tremendous new powers to manage and distribute information. However, these powers have not come without attendant dangers, problems and limitations. With the advent of E-Government, information systems now play an even more crucial role in the delivery of services and products to our customers.

As "trustee" of electronic assets, Maricopa County is responsible for operating, maintaining, and preserving technology resources to insure that they meet all business availability requirements. To overcome unforeseen interruptions to information systems, departments should develop formal recovery plans and be prepared to implement them.

The goal of this policy is to insure that Maricopa County agencies are able to continue IT-dependent business operations during and after a serious service interruption or disaster.

The principal priorities of disaster recovery planning are:

- To identify potential man-made or natural disasters
- To respond rapidly and appropriately to disasters
- To protect personnel and facilities
- To save data, hardware, and software
- To limit initial and subsequent damage
- To resume critical processes and restore data

B. Policy

Each elected official and appointed department director shall establish their Disaster Recovery Plan(s) and practices sufficient to ensure that: 1) their information resources are protected, backed-up, and recoverable; and 2) that the integrity, availability, and reliability of all electronic assets are not compromised or affected.

Each department shall:

- Identify business operations or information technology resources that are at risk
- Develop and maintain plans that enable short and long term recovery of IT systems
- Include sufficient detail to enable full resumption of normal operations
- File plans with Emergency Management and the Office of the Chief Information Officer (OCIO)
- Comply with reviews of Internal Audit
- Train staff to efficiently and effectively execute Disaster Recovery Plans
- Test Disaster Recovery Plans and emergency procedures
- Track, record, and report all disaster recovery activities
- Respond to all public inquiries about such incidents

C. Scope

This policy is applicable to all departments and special districts within Maricopa County that operate, manage, or use information technology services to support critical business functions.

The scope includes but is not limited to:

- Organizations that operate and manage technology for their own use or for use by other departments

Maricopa County Policies and Procedures	Subject: Disaster Recovery	Number: A1602 Issue Date: 11-02
--	-----------------------------------	------------------------------------

- Organizations that purchase and outsource computer services or telecommunications services from other departments or commercial sources
- All systems including: 1) stand-alone, shared, and network attached computers; 2) voice, data, and video telecommunications equipment; 3) other ancillary information management systems

D. Authority and Responsibility

Elected Officials And Appointed Department Directors Shall:

- Adopt a department-specific Disaster Recovery Plan and submit a copy to Emergency Management and the Office of the CIO.
- Establish Disaster Recover Plans, policy, procedures, standards, and guidelines sufficient to ensure the recovery of business operations to provide those services and products required by their customers. Departmental standards, procedures and practices developed must be consistent with the Maricopa County Disaster Recovery template, tools or standards set forth within this policy.
- Assign a disaster recovery coordinator function within their department. The continuation of business operations with minimal interruption is a part of that individual's responsibility.
- Conduct disaster recovery awareness training for all their employees.
- Test the Disaster Recovery Plan periodically and update the plan as needed.

Internal Audit shall:

- Conduct department audits of Disaster Recovery Plans, policies, procedures, and standards.

The Office of the CIO shall:

- Work with Internal Audit to insure compliance by all departments in developing and maintaining their individual Disaster Recovery plans.
- Meet periodically to discuss status and progress on Disaster Recovery Plans or recent disaster recovery activities.
- Recommend and set the direction for the Disaster Recovery Plan template to be used within the County; continue to research other templates, tools, and industry directions in disaster recovery.

Departmental Disaster Recovery Coordinators shall:

- Develop the department Disaster Recovery Plan(s), maintain the plan(s), orient staff on the plan and coordinate periodic testing of the plan.
- Use the recommended Disaster Recovery Plan template to develop their organization's plan(s).

County Employees shall:

- Understand their department's Disaster Recovery Plan(s) and any role that they have in the activation of such plan(s).

E. Definitions

- "Availability" is the ability to access specific electronic information or resources within a specific time frame and the degree to which a system or component is operational and accessible when required for use.

Maricopa County Policies and Procedures	Subject: Disaster Recovery	Number: A1602 Issue Date: 11-02
--	-----------------------------------	------------------------------------

- "Business Continuation" is to bring the business back to a functioning state at an acceptable level. This may or may not be a fully operational process and may lack some of the availability metrics of the original business operation (like timeliness) and may not include all deliverables.
- "Business Resumption" is to bring a department or agency back to 100% normal operations following a major disaster or business interruption.
- "Contingency Plan" is a set of procedures and/or steps to get an environment (technology or business) up and running as soon as possible. The contingency may or may not be what would be the normal mode of operation.
- "Disaster Recovery Plan" is a set of procedures and/or steps to restore services or products from an unavailable state to an available state. A Disaster Recovery Plan can include contingency plans, business continuation plans, business resumption plans, and backup/restore plans. The Disaster Recovery planning process includes documentation, plans, policies, procedures, standards, and/or guidelines that may be required to restore normal operation from a disaster or unplanned event.
- "Electronic Information" is data and information generated, stored, and/or transmitted by information systems.
- "Electronic Asset" is hardware, software, or data/information within a technology infrastructure.
- "Information System" is any mechanism used for acquiring, filing, storing, distributing, and retrieving an organized body of data. Information systems can include hardware, software, and firmware. It can also include any equipment or interconnected system or subsystems used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.
- "Integrity" is the quality (accuracy, precision, consistency, reliability) and time dependent state (current, historic, archive) of data or systems required by the business to meet its present and future goals.

F. Templates(s)

- The Disaster Recovery Plan template recommended by the OCIO can be found at the following location: <http://ebc.maricopa.gov/OET/library.aspx>. Select the *Disaster Recovery Plan* document.