CALIFORNIA JUDICIAL BRANCH

How to Use the Disaster Recovery Framework

A Guide for the California Judicial Branch

VERSION 1.4

OCTOBER 12, 2017

JUDICIAL COUNCIL
OF CALIFORNIA
INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

Table of Contents

1.0 INTRODUCTION

This "How to Use" guide acts as a reference for Judicial Branch Entities (JBE's) to assist them with establishing local policies and procedures based upon the Disaster Recovery Framework published by the Information Technology Advisory Committee, and the Judicial Council respectively. Since the framework was developed to establish a baseline disaster recovery approach at the branch level, this guide identifies the core purposes and sections of the Disaster Recovery Framework documents that are most relevant to JBE's. JBE's are not required to implement the framework in its entirety, rather the intent is to encourage JBE's to use the framework as a template to develop disaster recovery strategies and procedures appropriate to their unique local business requirements. It is intended to be used as a guide, not a benchmark, of what should be done.

This guide is intended to provide a roadmap for JBE's and does not include all the details required for implementing specific local backup and disaster recovery strategies and procedures. JBE's should refer to the complete framework document for specific recommendations and best practices.

2.0 BACKGROUND

The Information Technology Advisory Committee-sponsored Disaster Recovery Workstream was charged with accomplishing the following:

- Develop model disaster recovery guidelines, standard recovery times, and priorities for each of the major technology components of the branch.
- Develop a disaster recovery framework document that could be adapted for any trial or appellate court to serve as a court's disaster recovery plan.
- Create a plan for providing technology components that could be leveraged by all courts for disaster recovery purposes.

The formation of the workstream was based on a disaster recovery tactical initiative as identified in the Judicial Branch Technology Tactical Plan (2014-2018) aligning to the branch strategic goals, shown below in Figure #1.

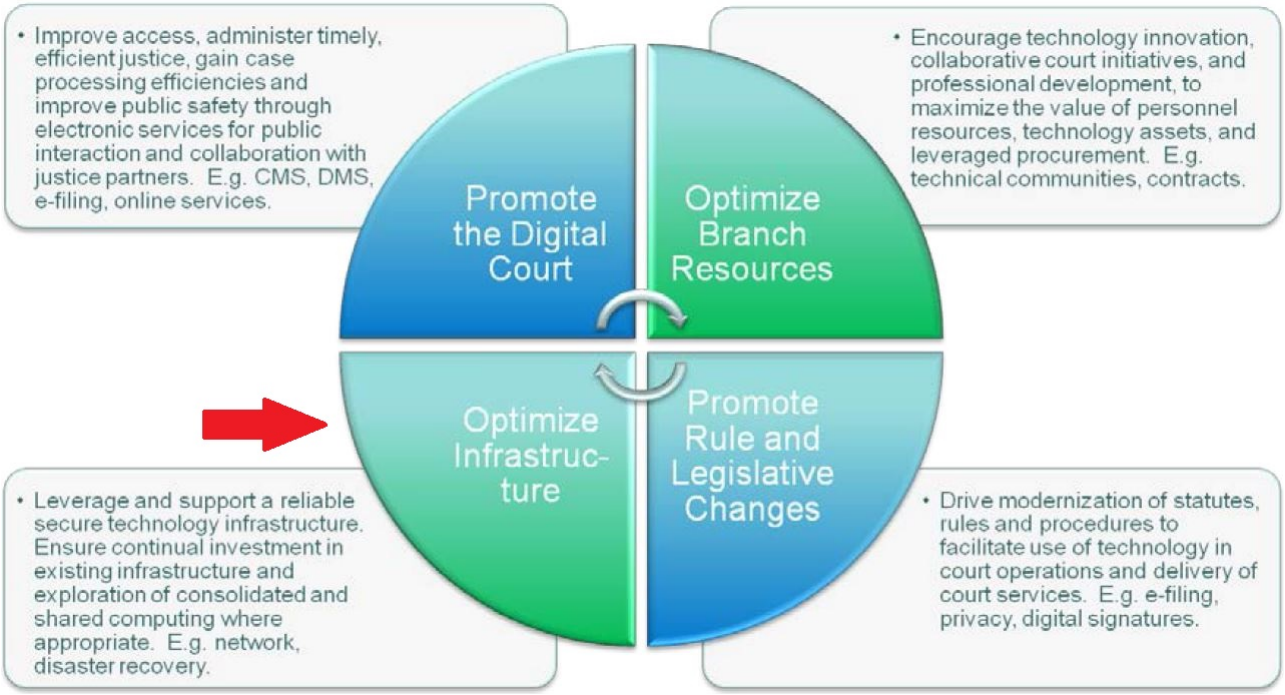

Figure 1: Judicial Branch Strategic Plan (2014-2018) Relevance

3.0 DISASTER RECOVERY FRAMEWORK

3.1 SCOPE

The disaster recovery framework has been developed for the establishment of a comprehensive and standard disaster recovery approach within the Judicial Branch of California. In order to produce the framework, input was solicited from multiple JBE's ranging from small to large in size so that a comprehensive framework could be developed that is suitable to all entities within the judicial branch. The framework is designed to set a direction, identify and address areas of concern expressed by entities within the judicial branch, and document policies and practices that can assist JBE's with their concerns by providing a framework for creating entity-specific disaster recovery plans and procedures, while following baseline recommendations and standards outlined accordingly.

The goals of the framework are:

- To suggest an overall direction and format for establishing and maintaining a disaster recovery plan. The plan helps JBE's ensure that their plan is comprehensive, consistent with other JBE's, and provides a baseline from which to work.
- To provide a holistic disaster recovery framework that the JBE's can leverage to help streamline and expedite the completion of disaster recovery planning unique to each JBE.

- To provide general baseline recommendations on data recovery times, standards and approaches to disaster recovery.

- To provide suggestions for technology solutions (hardware/software) both in-place and not-in-place within the Judicial Branch that meet the requirements for implementing a disaster recovery plan.

- To satisfy courts' needs to establish disaster recovery plans around modern hosting services such as cloud, including software as a service, infrastructure as a service, etc. Modern hosting solutions are drastically changing the way courts manage and protect electronic data, therefore necessitating agile and proven methods on how to ensure data is backed up and to support the high availability of systems.

3.2 ORGANIZATIONAL CHARACTERISTICS

The framework establishes how disaster recovery plans should be created and maintained within individual judicial branch entities. It is imperative that a JBE's disaster recovery plan(s) and objective(s) align to—at a minimum, and satisfy the rules of court as related to data retention and privacy. Because JBE's have differing and unique relationships with how data is shared and/or divided with other justice partners, careful consideration should be exercised to ensure that both sides are taking data protection into account, ensuring that disaster recovery policies impacting each other are clearly outlined and communicated and regularly validating that all business-critical data is protected from a data backup perspective. Therefore, disaster recovery policies and procedures (administrative and technical) related to each JBE and respective justice partners are of particular importance.

3.3 DOCUMENTATION STRUCTURE

A disaster recovery plan is supported by a collection of documentation capturing differing levels of detail while maintaining consistent guidance for all participants. A JBE's disaster recovery plan documentation portfolio should consist of the following categories of documents:

- **Organizational Policy** – Expresses management's expectations with regard to tolerance to data loss for various classes of data and expectations for recovery times and retention. Generally limited to identification of base principles, including roles and responsibilities, and the disaster recovery framework. This framework provides the organizational policy for individual judicial branch entities.

- **Implementing Policy** – Further refines management's expectations; usually issued by a subordinate business or organizational unit for the purpose of interpreting the organizational policy to local entity practices. These policies will be developed as needed by the local entity.

- **Standards** – Identify specific hardware and software features and products whose use has been determined to be in support of policy and aligned to fulfilling the entities disaster recovery mission. Standards may be established by local entities as needed to support policy objectives and to streamline operations.

- **Procedures** – Support standards and policy by providing step-by-step instructions for the execution of a disaster recovery process. Judicial branch entities will develop and document procedures to ensure the quality and repeatability of disaster recovery processes.

- **Guidelines** – Provide recommendations which can be used when other guidance has not been established. Guidelines are usually created at lower operational levels such as departments to address immediate needs until consensus is reached on broader direction.

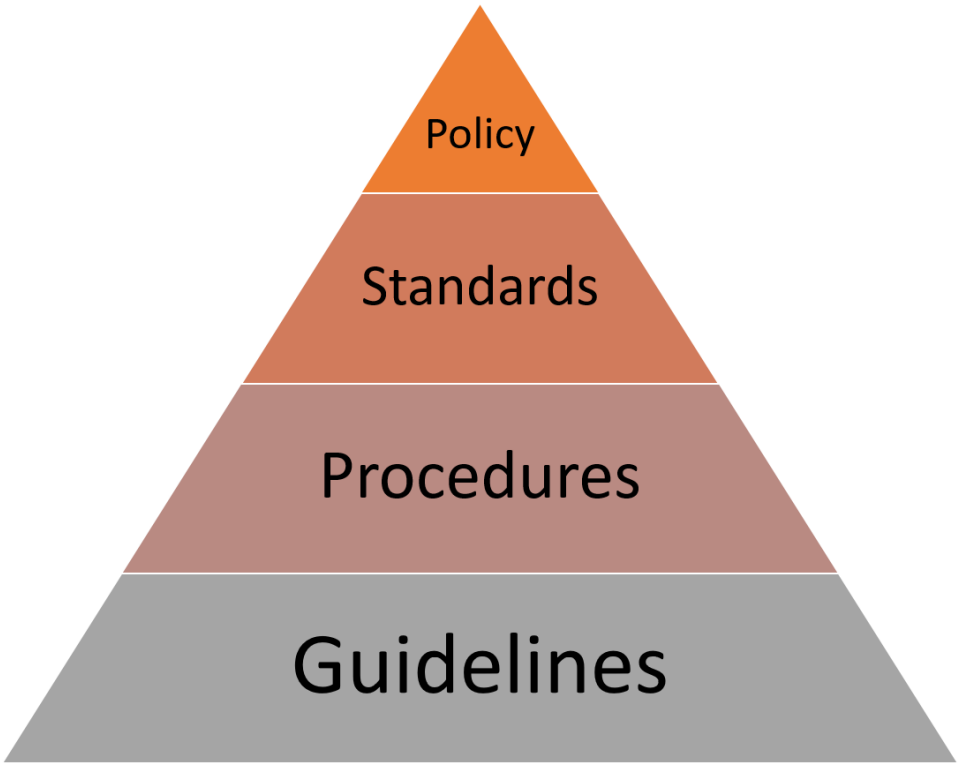

Figure 2: Documentation Structure

The following documents, published 08/1/2017 shall serve as the official Disaster Recovery Documents Package for the California Judicial Branch. This package represents “best practices” and is recommended as a disaster recovery framework to be used by all judicial branch entities.

1. Document (Reference): How to Use Guide (this document)

2. Document (Reference): Recommendations & Reference Guide

3. Document (For Completion by JBE): Adaptable Disaster Recovery Template

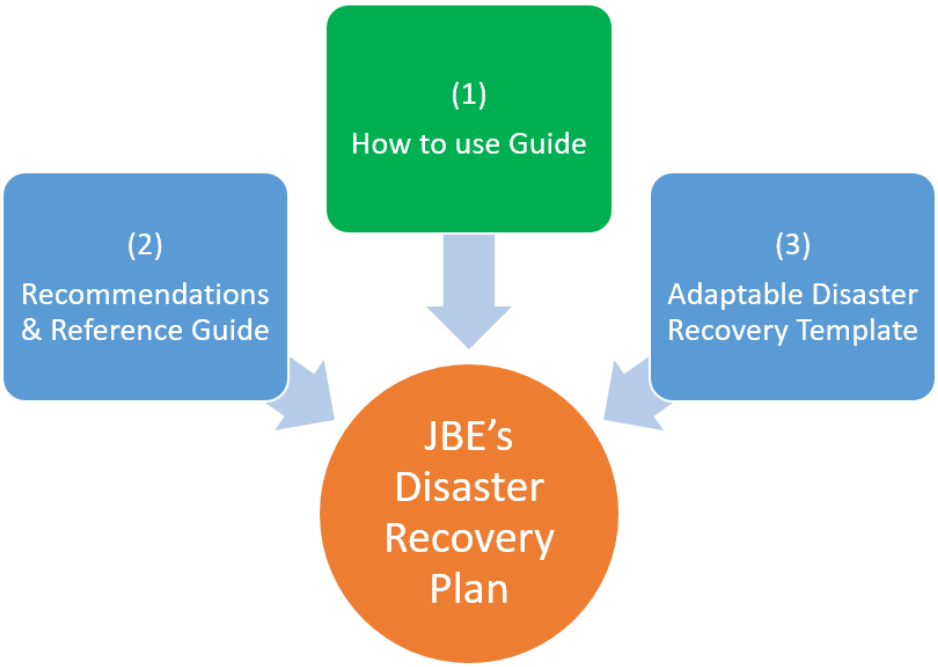

Figure 3: Document Path to Disaster Recovery Plan

4.0 PURPOSE OF DISASTER RECOVERY

Information and the supporting processes, systems, and pockets of data are important assets. Defining, achieving, maintaining, and improving disaster recovery systems, approaches and readiness may be essential to maintain legal compliance, integrity, and availability of information and systems.

JBEs and their information systems and data are faced with security threats and chances of corruption and/or loss from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage (such as malicious code, computer hacking, and denial of service attacks) have become more ubiquitous, more ambitious, and increasingly sophisticated. Ultimately, the consequences are felt the heaviest when data and systems are unreachable and/or data has been lost and/or compromised.

Many information systems have not been designed with disaster recovery in mind. While some systems do have means and methods to ensure that data is protected, the entities responsible for those systems must ensure that those means and methods are implemented and routinely tested.

Methods on protecting data that can be achieved through technical means are plentiful, and should be supported by appropriate management policies and procedures, including adequate funding and/or resource allocation. Identifying which controls should be in place requires careful planning and attention to detail. Disaster Recovery management requires, at a minimum, participation by all employees in the branch. It may also require participation from local and state justice partners, the public suppliers, third parties, contract labor, or other external parties. Disaster Recovery is a continually evolving area and courts are encouraged to stay informed and educated on current methods, products and technologies and ensure procedures are updated along the way. Although there is no requirement, it is also a best practice to establish an escalation path to ensure that incidents receive the proper attention based on severity and are processed in a timely manner.

Data is an asset, which, like other important business assets, has value to an organization and consequently needs to be suitably protected. JBE's, as part of their on-going program to maintain adequate and effective controls, want to ensure that the various systems and pockets of data scattered throughout the organization are accounted for and protected adequately. The benefits of keeping data as centralized as possible within various identified areas/systems/datacenters significantly outweighs scattering data across the organization especially beneath the core datacenter layer. A JBE's disaster recovery posture and approach should emanate from the IT Department and administrative body, but never delegated to end-users. Additionally, ongoing education to end-users is essential to ensure that unseen data mines are not being created and stored in areas where IT does not have routine visibility and therefore may not get included in the respective disaster recovery plan.

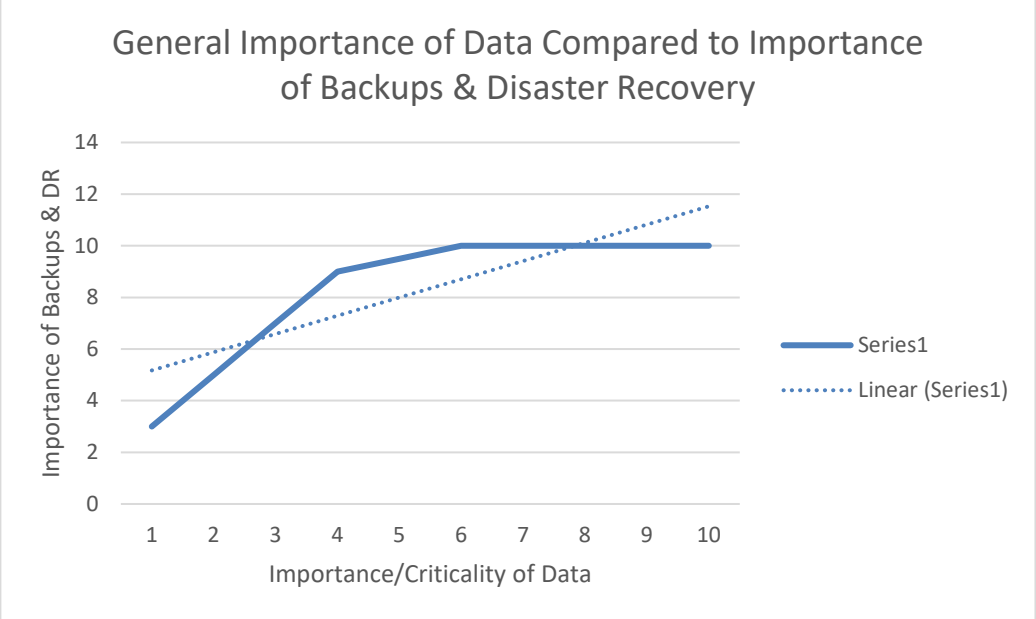

Figure 4: Importance of Data Compared to Importance of Backups & Disaster Recovery

5.0 USING THE FRAMEWORK

The Disaster Recovery Framework published by the Judicial Council provides a model that JBE's can leverage. JBE's are not required to implement the recommendations contained in the framework but they are encouraged to leverage the framework as appropriate for their unique local business requirements. The framework provides context for a court's local IT disaster recovery plan. The framework is designed to be modular and expandable so that courts can refer only to the sections that are relevant to them and expand accordingly based on varying needs. The framework references and recommends specific technologies known to be in use already within the Judicial Branch that can be implemented and shortening a JBE's effort in researching solutions.

A local court can utilize the framework and this "how to use" guide in the following manner:

1. The JBE has prioritized an initiative to improve the JBE's disaster recovery strategy and solution. Initiating such an effort will require staff time, resources and executing the initiative after solution(s) have been decided upon will ultimately require a financial commitment from the JBE for hardware/software and potential professional services.

2. Review this "how to use" guide and determine which stakeholders will be included in the development of the JBE's IT disaster recovery plan in order to create a project execution team.

3. The team then reads the "Recommendations & Reference Guide" to obtain a clear understanding of recommended standards, backup strategies, approaches to disaster recovery and various solutions being promoted that are in use today by various JBE's.

4. The JBE identifies options for implementing the plan.

5. The JBE determines what funding and resources exist to implement the local policy.

6. The JBE implements any hardware/software solution(s) needed to fulfill the disaster recovery plan and objective(s).

7. The JBE then completes the "Adaptable Disaster Recovery Template" to produce it's local Disaster Recovery Plan.