THE STATE BAR
OF CALIFORNIA

OFFICE OF LEGAL SERVICES
Standing Committee on the Delivery of Legal Services
2012-2013 Chair, S. Lynn Martinez, Los Angeles

180 Howard Street, San Francisco, California 94105
Telephone (415) 538-2267 Fax (415) 538-2552

Steps to Disaster Planning for Legal Services Providers

After a disaster, the main goal is to resume operations and serve clients again as quickly as possible. The goal of disaster planning is to define what a disaster means to your staff and program, and develop approaches and safeguards to ensure that, after a disaster, staff members are safe, services are available, and data, property, and other assets are protected.

Recovery goals:

- Protect safety of personnel
- Protect safety and security of vital assets, documents, and information
- Resume basic client services
- Return to normal operations

Step 1: Form a disaster planning team.

A legal services provider can have numerous and diverse operations. A diverse team of directors, managers, staff, and volunteers can help analyze these complex operations to identify the preparations needed to ensure that the organization can resume full function after a disaster or at least protect key valuables. Organizations operating multiple sites should include appropriate representation from each location.

Step 2: Assess risks and evaluate potential hazards.

Risk assessment is the process for defining a program's tolerance for, and definition of, a disruption in operations or loss of critical data. By identifying potential events that would result in massive work disruption or data loss – whether localized to your own organization or consequent of a broader community event, – you can evaluate the problems likely to arise from such events, their severity, and the most effective response. Consider risk assessment needs for technology and technical systems, but also for work life in general.

- Identify your organization’s mission, goals, and objectives in general.
- Identify essential functions of your organization *(see Sample Form 2)*.
- Perform a Business Impact Analysis *(see Sample Form 3)* to identify possible points of failure in the execution of the essential processes, determine the impact of such failures, and create alternatives or remedial strategies.

Evaluating potential hazards involves reviewing any disasters that have already occurred in your organization's history, as well as reviewing what is possible and how those hazards might affect your organization. Try to identify a few situations that would put your organization most at risk. Keep in mind the likelihood of the risk, the threat to life and safety, and the cost of mitigating that risk. Possible hazards may include:

- Internal Disasters: Systems failures, medical emergencies, workplace violence, building decay, personnel loss.
- External Disasters: *Environmental* – Earthquake, hurricane, tornado, severe storm, fire, flood, drought, lightening, landslides, wind damage; *Non-Environmental* – Civil unrest, terrorism, bomb threat, utilities disruption, hazardous material incident.
- Man-Made Disasters: Security breach or sabotage, theft.

Step 3: Minimize risk.

For each potential risk, identify the policies and systems you already have in place, or could implement to mitigate them.

- Inventory and evaluate emergency supplies and equipment currently on hand.
- Develop evacuation routes and procedures or implement building's evacuation route *(see Sample Forms 4-5)*.
- Consider preventative structural maintenance or supply upgrades, such as purchasing fire- and water-proof filing cabinets, ensuring alternate power sources for critical necessities; checking the building's structure for problems; ensuring the fire alarm and sprinkler systems work, etc.
- Photograph and inventory all office furnishings, electronics, hardware, software licenses and installation discs, reference materials, supplies, etc. and arrange to store valuables off-site *(see Sample Form 6)*.
- Review and evaluate insurance policies and arrange for a disaster line of credit with your bank representative *(see Sample Form 7)*.

Step 4: Safeguard your digital network and case management system.

Information security does not have a one product, one-size-fits-all solution. It is best to implement the necessary security solutions to common threats while remaining vigilant to new dangers. Be proactive in taking steps to safeguard yourself, your program, and your clients.

- Keep your operating system (OS) up-to-date.
- Install/update firewalls, anti-virus, anti-spyware, and intrusion detection software.
- Secure all computers and network access, i.e., passwords, thumbprint readers.
- Secure wireless networks, i.e., reset administrator password, disable SSID broadcast, limit number of computers, place in center of building, set to infrastructure mode, limit access by MAC address, disable DHCP, and assign static IP addresses.
- Implement a document security policy, i.e., password protection, and secure pdf files.
- Implement an email usage policy, i.e., encryption, disclaimers, spam filters, and storage and retention.
- Implement an internet usage policy, i.e., restrict pop-ups.
- Implement daily back-up procedures and ensure safety of back-up material, i.e., automatic back-up, off-site storage, and encryption.
- Install remote data wiping, encryption software, and anti-theft protection on all portable devices (smart phones, PDAs, laptops, USB drives).

- Implement similar security measures on all computers (personal, home, laptops) employees use to access the organization’s network and data.
- Wipe clean all discarded electronic devices.

Step 5: Identify potential consequences of each hazard or disaster and work to address them.

Find out what actually happens in your organization every day.

- **What information is most critical?** Identify the important information that each department (Accounting, Human Resources, Information Technology, Legal, etc.) needs to be operational and ensure that someone can access that information in the event of a disaster *(see Sample Form 8)*.
- **What is your program's tolerance for disruption or data loss?** Your program should be able to articulate what constitutes a disaster and when to initiate the disaster plan to resolve any system disruption.
- **Have you defined your Recovery Time Objectives?** For each critical operation, identify your "Recovery Time Objective" – the amount of time between when a disaster is declared and when an application or operation needs to be restored *(see Sample Forms 2-3)*. Think about how long you can sustain operations (or non-operations) in a disaster, and the potential consequences of a diminished client base. Prioritize the recovery of operations based on the importance of each operation to your organization’s wellbeing and survival, i.e. how long your organization can survive without this operation in place. Also ensure there is sufficient funding (including petty cash) to sustain your program for a period during recovery of data or operations.

Step 6: Develop recovery strategies for disasters.

With the groundwork done, you can think about what strategies you need to respond to disasters appropriately. This will involve getting the work environment and area up and running as well as the technology. You will also want to consider organizational continuity – how to serve clients in case of a disaster, and how priorities will shift in a disaster.

- Make a list of emergency equipment, including location of equipment and floor plans, and prepare emergency kits for general survival and office supply kits for off-site operations.
- Prepare contact lists for staff, volunteers, board members, emergency response agencies, property agents, recovery vendors, clients, and consultants *(see Sample Forms 9-12)*.
- Develop a communication plan to alert all personnel, clients, local media, funders, government agencies, and partner organizations of the disaster *(see Sample Form 13)*. Include any necessary translations of advisory messages. Make sure communication system is up-to-date.
- Assemble a list of vital records for business continuity; including records concerning both the legal and financial rights of the organization and its personnel, and the continuation of essential processes *(See Sample Form 14)*.
- Identify and secure an alternative workspace(s) and the essential resources your organization needs to recover essential operations *(see Sample Form 15)*. Keep in mind you may need to relocate different functions to different workspaces, or it may be easiest to utilize remote access for certain functions. After you secure an alternative workspace, make sure you can access your back-up data from that site and test restoring the data.

- Establish memorandums of understanding with bar associations, other legal services providers, law firms, and community organizations for emergency use of space, resources, volunteers, etc.
- Prepare a Business Continuity Plan that describes how your firm intends to return to serving clients and carrying out critical business processes after a disaster occurs, including assessing the status of employees, workspaces and resources, defining steps to recover essential business processes, and, in the event of a community-wide disaster, anticipating disaster-related legal needs of new and existing clients.

Step 7: Develop written disaster plan.

It is important to have a written disaster plan for the program and to coordinate with the community, such as state and regional disaster organizations and local Voluntary Organizations Active in Disaster (VOAD), prior to a disaster and as part of the planning process. Your plan should consider:

- Staff protection and safety
- Internal communication
- How to protect business assets
- What must remain operational
- What to do about office space, property, technology, and data
- Insurance requirements and claim procedures
- How to get back to serving clients (Business Continuity Plan)
- Vendors that can help with recovery
- Coordination with local, state, and federal emergency response agencies

Step 8: Develop a disaster team.

Once a plan is in place, you will need to identify individuals who will be taking charge in the event of a disaster (*see Sample Form 1*). Designate one person to be in command in the event of a disaster and designate an alternate. Determine what each person on the disaster team will be responsible for before, during and after a disaster, i.e., section of a building, department, contacting staff, contacting clients, recovering documents, etc.

Step 9: Advise staff, test it, and keep it current.

Plans are worth their time only if they work. Train your staff and volunteers regularly, make disaster preparation part of the everyday landscape, do walkthroughs, enforce, and review on a regular basis.

Sample Disaster Planning Forms

Each organization’s circumstances and structures are unique. You will need to tailor the forms below to meet your organization’s need. To complete this working plan, staff members will need to work together to “fill in the blanks,” delete and add sections that are applicable, and expand sections where needed.

Sample Form 1: Disaster management team.

Name	Position	Phone Number	Alt. Phone Number	Email Address	Area of Responsibility
					Person in Command/ Decision to Activate Plan
					Second in Command
					Admin/Operations
					Finance/Accounting
					Communications/ Development
					Human Resources
					Information Technology
					Legal
					Client Services
					Other

Sample Form 2: List of critical functions (in order of importance).

Function	Recovery Time Objective	Alternatives Until Restored	Primary Person Responsible	Secondary Person Responsible

Sample Form 3: Business impact analysis.

Department	Manager	Process	Vital Records	External Vendors	Resource Requirement	Recovery Time Objective

Sample Form 4: Evacuation plan (attach a list of all office staff to be accounted for).

- Person in charge of evacuation:
- Warning System:
- Assembly Site:
- Alternate Site:

Sample Form 5: Known persons in need of special assistance.

Name of Person	Location	Type of Assistance Required	Person Responsible for Providing Assistance

Sample Form 6: Software inventory.

Software	Number of Licenses	Version	Product Key	CD Location	Notes

Sample Form 7: Insurance information.

Policy Type	Policy Number	Agent	Contact Information

Sample Form 8: Access to secure information.

Information	Primary Person with Access	Phone Number/ Email	Secondary Person with Access	Phone Number/ Email

Sample Form 9: Personnel and board contact information chart.

Name/Title	Home Address	Work/Home/ Cell Phone	Email/ Alt. Email	Emergency Contact Name	Emergency Contact Phone Number

- Location of Telephone Tree:
- Emergency Website/Voice Message:
- Person Responsible for Updating:

Sample Form 10: Local direct service organizations.

Organization	Location	Phone Number	Service Provided
Emergency Services			
Red Cross			Disaster Relief
FEMA			
State Office of Emergency Mgmt			
County Office of Emergency Mgmt			
Department of Health and Human Services			
Center for Disease Control			
County Mental Health Crisis Hotline			
County Referral Services			
Department of Transportation			
Small Business Administration			
			Food Bank
			Shelter
			Crisis Center
			Community Center

Sample Form 11: Services needed in emergency.

Company	Service	Contact Person	Phone Number	Account Number	Email
	Building Management				
	Building Security				
	Janitorial				
	Maintenance				
	Mechanical				
	Police				
	Fire				
	Ambulance				
	Public Works				
	Poison Control				
	Hospital or Urgent Care				
	Pharmacy				
	Electric Company				
	Gas Company				
	Telephone Company				
	Water Company				
	Hazardous Waste				
	Electrician				
	Plumber				
	Contractor				
	Locksmith				
	Insurance Company				
	Mass Care Facility				

	Computer Recovery				
	Document Recovery				
	Website Coordinator				
	Language Line Service				
	Supermarket				
	Other				

Sample Form 12: Crucial contacts & key service providers.

Company	Service Provided	Contact Person	Phone Number	Email Address
	Vital Records Recovery			
	Hot Site			
	Payroll			
	Health Insurance			
	Employee Assist. Program			
	Benefits Admin			
	Legal Counsel			
	Chamber of Commerce			
	Accountant			
	Bank Representative			
	Creditor			
	Online Credit Card Processor			
	Software			
	Office Supplies			
	Copy Machines			
	Printer Repair			
	Mail Meter			
	Truck Rental			

Sample Form 13: Media and community contacts.

Organization	Contact Name	Phone Number	Email Address	Relationship
				Newspaper
				Television Station
				Radio Station
				Superior Court
				County/Local Bar Association
				Other Legal Services Providers
				Partner Agencies
				Funders

- Designated Spokesperson:

Sample Form 14: Critical documents (Keep a hard copy and electronic copy of as many documents as possible in a central location for easy access in a disaster).

Document	Location	Location of Copies	Person Responsible	Issuing Organization	Contact Info
Incorporation Papers					
Tax Documents					
Mission Stmnt/ Priorities					
Bylaws					
Branding Documents					
Organizational Chart					
Job Descriptions					
Financial Statements					
Accounting/ Budget Rcrds					
Bank Account Info/Checks					
Contracts					
Insurance Policies & Info					

Payroll Records					
Employee Records & Info					
Volunteer Records & Info					
Board Member Records & Info					
Partnership Agmnts/MOUs					
Grant/Donor Documents					
Evaluation Reports					
Client Info & Documents					
Court Documents					
Computer Back-up					
Software Passwords					
Equipment Inventory					
Vendor Records					
Deeds					
Leases					
Translated Disaster Msgs					

Sample Form 15: Alternative work location(s)

Location Name	Address	Access/ Security	Directions from Office	Description of Space	Technology Available	Resources Needed

- Tele-working/Remote Access Arrangements:

Resources:

American Bar Association Committee on Disaster Response and Preparedness
www.americanbar.org/groups/committees/disaster.html

- Security, Computer Backup, and the Cloud
- Surviving a Disaster: A Lawyer's Guide to Disaster Planning - August 2011

American Red Cross
www.redcross.org

- Personal Workplace Disaster Supplies Kit
- Preparing Your Business for the Unthinkable

CERT: Community Emergency Response Teams
www.citizencorps.gov/cert

Collaborating Agencies Responding to Disasters
www.cardcanhelp.org

- Workplace Hazard Mitigation Checklist
- Prepare to Prosper: 9 Small Steps that Reap Huge Rewards

Commander Navy Installation Command
www.cnic.navy.mil/CNIC_HQ_Site/index.htm

- Operation Prepare: Emergency Kits

Council on Foundations
www.cof.org

- Disaster Preparedness and Recovery Plan

Lawyers' Professional Indemnity Company
www.lawpro.ca

- Managing Practice Interruptions
- Managing the Security and Privacy of Electronic Data in a Law Office

TechSoup Global
www.techsoupglobal.org

- The Resilient Organization: A Guide for Disaster Planning and Recovery

United States Department for Homeland Security (FEMA)
www.ready.gov

- Business Continuity Plan
- Emergency Response Plan

United States Department of Labor, Occupational Safety & Health Administration
www.osha.gov

- Emergency Action Plan Checklist

United States National Archives and Records Administration
www.archives.gov

- Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide

This resource document was prepared by the State Bar of California's Standing Committee on the Delivery of Legal Services (SCDLS) and the Office of Legal Services. For more information or to provide feedback, contact Sharon Ngim at sharon.ngim@calbar.ca.gov and Jennifer Kregear at jennifer.kregear@calbar.ca.gov.