# [INSERT FIRM LEGAL NAME]
# Disaster Recovery Policy

**[Insert Firm Logo]**

**Version 1.0**
**[Insert Date]**

[Insert Firm Logo]

# Contents



## Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company specific document. Otherwise, it would be a liability exposure to establish a policy and not to comply with it.

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

**Delete the instructions after finalizing and adopting the policy.**

## Disaster Recovery Overview

Disaster recovery is the process of restoring critical technology services used to support business operations immediately following a significant man-made or natural disruption (“disaster”).

Critical technology services are identified by the organization through formal and/or informal business impact analyses (BIA), and include technology issues such as connectivity, cloud services, network infrastructure, servers, applications, and a limited number of client systems.

The disaster recovery process is established from many supporting recovery processes, and often organized into a disaster recovery plan (DRP). In the greater context of recovery, the DRP supports the broader and longer term strategy found in a business continuity plan (BCP). Disaster recovery applies to technology and shorter term disruptions, whereas business continuity applies to most, if not all business processes over an extended period of time

## Purpose

The purpose of the **[Insert Firm Legal Name]** Business Continuity and Disaster Recovery Policy is to provide direction and general rules for the creation, implementation, and management of the **[Insert Firm Legal Name]** Disaster Recovery Plan (DRP).

## Audience

The **[Insert Firm Legal Name]** Disaster Recovery Policy applies to individuals accountable for ensuring a disaster recovery plan is developed, tested, and maintained.

## Policy

- **[Insert Firm Legal Name]** must create and implement a Business Continuity and Disaster Recovery Plan ("BDRP").
- The DRP must be periodically tested and the results should be used as part of the ongoing improvement of the DRP.
- The DRP, at a minimum, will identify and protect against risks to critical systems and sensitive information in the event of a disaster.
- The DRP shall provide for contingencies to restore information and systems if a disaster occurs. The concept of disaster recovery includes business resumption.
- **[Insert Firm Legal Name]** disaster recovery planning must ensure that:
    - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
    - personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated;
    - documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.
- The **[Insert Firm Legal Name]** DRP must include at a minimum, the following elements:
    - Business impact analysis, including risk assessment, Information Resource asset classification, and potential disruption to stakeholders
    - A classification system to identify critical systems and essential records
    - Mitigation strategies and safeguards to avoid disasters. Safeguards should include protective measures such as redundancy, fire suppression, uninterruptible power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature, or humidity
    - Backups and offsite storage
    - Information Resource role in business resumption
    - Contingency plans for different types of disruptions to Information Resource and systems availability
    - Organizational responsibilities for implementing the disaster recovery plan
    - Procedures for reporting incidents, implementing the disaster recovery plan, and escalating **[Insert Firm Legal Name]**'s response to a disaster
    - Multiple site storage of back-up documents
    - Training, testing, and improvement
    - Annual review and revision

## Definitions

**Cloud Computing Application:** Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Common examples of cloud computing applications are Dropbox, Facebook, Google Drive, Salesforce, and Box.com.

**Confidential Information:** Confidential Information is information protected by statutes, regulations, **[Insert Firm Legal Name]** policies or contractual language. Information Owners may also designate Information as Confidential. Confidential Information is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis only. Disclosure to parties outside of **[Insert Firm Legal Name]** must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Information include:

- Customer data shared and/or collected during the course of a consulting engagement
- Financial information, including credit card and account numbers
- Social Security Numbers
- Personnel and/or payroll records
- Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
- Any Information belonging to an **[Insert Firm Legal Name]** customer that may contain personally identifiable information
- Patient information

**Incident:** An incident can have one or more of the following definitions:

- Violation of an explicit or implied **[Insert Firm Legal Name]** security policy
- Attempts to gain unauthorized access to a **[Insert Firm Legal Name]** Information Resource
- Denial of service to a **[Insert Firm Legal Name]** Information Resource
- Unauthorized use of **[Insert Firm Legal Name]** Information Resources
- Unauthorized modification of **[Insert Firm Legal Name]** information
- Loss of **[Insert Firm Legal Name]** Confidential or Protected information

**Information Resource:** An asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can be stored in many forms, including: hardware assets (e.g. workstation, server, laptop) digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.

**Internal Information:** Internal Information is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Information is information that is restricted to personnel

designated by **[Insert Firm Legal Name]**, who have a legitimate business purpose for accessing such Information.

Examples of Internal Information include:

- Employment Information
- Business partner information where no more restrictive confidentiality agreement exists
- Internal directories and organization charts
- Planning documents

**Mobile Device**: Computing devices that are intended to be easily moved and/or carried for the convenience of the user, and to enable computing tasks without respect to location. Mobile devices include, but are not necessarily limited to mobile phones, smartphones, tablets, and laptops.

**Penetration Test**: A highly manual process that simulates a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment.

**Personally-owned**: Systems and devices that were not purchased and are not owned by **[Insert Firm Legal Name]**.

**Public Information:** Public Information is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public Information, while subject to **[Insert Firm Legal Name]** disclosure rules, is available to all **[Insert Firm Legal Name]** employees and all individuals or entities external to the corporation.

Examples of Public Information include:

- Publicly posted press releases
- Publicly available marketing materials
- Publicly posted job announcements

**Removable media:** Portable devices that can be used to copy, save, store, and/or move Information from one system to another. Removable media comes in various forms that include, but are not limited to, USB drives, flash drives, read/write CDs and DVDs, memory cards, external hard drives, and mobile phone storage.

**Vulnerability Scan**: A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.

## Waivers

Waivers from certain and specific policy provisions may be sought following the **[Insert Firm Legal Name]** Waiver Process.

## Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

## Revision Table

| Revision History | | | | |
|---|---|---|---|---|
| **#** | **Version #** | **Date** | **Updates/Changes** | **Owner** |
| **1** | 1.0 | September 2022 | Initial Draft | Riskigy |
| **2** | | | | |