**Name of Organization**

**Disaster Recovery (DR) Requirements – Industries**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) DR Run Book Industries is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. All Industries 5](#_Toc87538059)

[II. Financial 5](#_Toc87538060)

[III. Healthcare 6](#_Toc87538061)

[IV. Government 7](#_Toc87538062)

The purpose of this document is to highlight the requirements for all key industries related to IT Disaster Recovery. This document should be reviewed and updated annually.

# All Industries

**Sarbanes-Oxley Act (SOX)**

* Corporate officers are liable for business continuity
* Relevant for publicly held companies in the U.S.

**Internal Revenue Service (IRS) Procedure 86-19**

* Requires off-site protection and documentation of computer records of tax information
* Records must be available if the primary facility is subjected to unplanned outage

**Consumer Credit Protection Act (CCPA) Section 2001 Title 1X**

* Due diligence for availability of data in Electronic Funds Transfers including Point of Sale

# Financial

**Expedited Funds Availability (EFA) Act, 1989**

* Federally chartered financial institutions must have demonstrable business continuity plans to ensure prompt availability of funds

**Gramm-Leach-Bliley Act (GLBA) 1999**

* Institutions are required to implement a written information security program that includes admin., tech., and physical safeguards.

**Basel II, Basel Committee on Banking Supervision (BCBS) 2003**

* Requires that banks put in place Business Continuity (BC)/DR plans to ensure continuous operations and limit losses.

**Federal Financial Institutions Examination Council (FFIEC)**

* Specifies that Board of Directors is responsible for ensuring that a comprehensive BC plan has been implemented

**FFIEC Inter-Agency Policy 1997**

* Requires any service bureau or outsourcing companies that service banks to have in place Business Continuity plans

**FFIEC Financial Institution Letter (FIL) 67-97/82-96**

* Requires Board of Directors to ensure that a comprehensive business resumption and contingency plan has been implemented, to encompass distributed computing and external service bureaus.

**Bulletin R-67: Federal Home Loan Bank**

* Follows the intent of BC177 which required documented, exercised, and maintained recovery plans for all user environments and business functions.

**Securities and Exchange Commission (SEC) 17 CFR 240 (2005)**

* SEC regulations require that financial transaction histories be maintained for all electronic securities transactions, and backup power be in place to maintain continuity. This regulatory requirement is mandatory for applicable entities.

**Financial Industry Regulatory Authority (FINRA) Rule 4370**

* Applies to all FINRA members
* Rule 4370 — FINRA's emergency preparedness rule — requires firms to create and maintain business continuity plans (BCPs) appropriate to the scale and scope of their businesses, and to provide FINRA with emergency contact information.

**New York Stock Exchange (NYSE) Rule 446 / National Association of Securities Dealers (NASD) 3510/3520 (2004)**

* Applies to all members and member organization of the NYSE or NASD
* Rule requires members establish and maintain business continuity strategies and plans relating to an emergency or significant business disruption. It also requires that members' plans be reasonably designed to enable it to meet its existing obligations to customers. This regulatory requirement is mandatory for applicable entities.

**Commodity Futures Trading Commission (CFTC) Rule 23.603**

* Applies to Swap Dealers (SDs) and Major Swap Participants (MSPs)
* The CFTC Rule 23.603 requires SDs and MSPs to establish and maintain a written business continuity and disaster recovery plan that outlines the procedures to be followed in the event of an emergency or other disruption of its normal business activities. The business continuity and disaster recovery plan should be designed to enable the swap dealer or major swap participant to continue or to resume any operations by the next business day with minimal disturbance to its counterparties and the market, and to recover all documentation and data required to be maintained by applicable law and regulation

# Healthcare

**Health Insurance Portability & Accountability Act (HIPAA) 1996**

* Requires data back-up plan, disaster recovery emergency plan, and emergency mode operations plans

**Food and Drug Administration (FDA) Code of Federal Regulations (CFR), title XXI, 1999**

* Requires BC measures to ensure availability of information
* Establishes the requirements for electronic records and electronic signatures

**HIPAA Code of Federal Regulations 164.308 (A)**

* Data backup plan (Required) Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
* Covered entities must establish and implement procedures to create and maintain retrievable exact copies of electronic health records and information. Specifically, the data backup must be frequent, offsite, the data must be recoverable, and data-at-rest must be encrypted. Your plan must also be documented and tested.

**HIPAA Code of Federal Regulations 164.308 (B)**

* Disaster Recovery Plan (Required) Establish (and implement as needed) procedures to restore any loss of data.
* Companies must have a central document that specifies the resources, technology, processes, personnel, and data required to protect and recover healthcare information in the event of a disaster.

**HIPAA Code of Federal Regulations 164.308 (C)**

* Emergency mode operation plan (Required) Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
* Companies must have a detailed plan for how they continue business operations and continue protection during an emergency. This could include accessing protected systems and workstations even in extreme circumstances.

**HIPAA Code of Federal Regulations 164.308 (D)**

* Testing and revision procedures (Addressable) Implement procedures for periodic testing and revision of contingency plans
* Companies must document and implement procedures for periodic testing and revision of contingency plans. This periodic testing is intended to discover weaknesses and revise documentation and processes as needed to address those weaknesses.

**HIPAA Code of Federal Regulations 164.308 (E)**

* Applications and Data Criticality Analysis (Addressable) Assess the relative criticality of specific applications and data in support of other contingency plan components
* Companies should understand the relative importance of each application and data in order to inform the contingency plan order of operations and processes, as well as special considerations.

# Government

**Government Continuity of Operations (COOP) and Continuity of Government (COG) Federal**

**Preparedness**

* Establishes requirements for BC plans and response readiness
* BC plans must be able to sustain operations for 30 days
* All BC plans must be maintained at a high level of readiness, must be capable of implementation without warning, must be operational within 12 hours of activation

**Federal Emergency Management Agency (FEMA) Federal Response Planning Guidance (FRPG) 01-94**

* All department and agency heads must formally plan for continuity of essential operations
* Written documents for BC must be maintained and current

**Federal Information Security Management Act (FISMA) 2002**

* Requires electronic data to be available during a crisis
* Emphasis of FISMA is on data security

**Governmental Accounting Standards Board (GASB) Statement No. 34 1999**

* Requires a BC/DR plan to ensure that agency’s mission continues in time of crisis
* Applies to all government entities that operate utilities.