

Syra Health Information Technology Disaster Recovery Overview

Syra Health customer and administrative data are important Company resources and assets. Data used by the Company often contains detailed information about Syra Health as well as personal information about Syra Health customers, staff, and other third parties affiliated with the Company. Maintaining availability of the data is paramount to operational success.

This document is to provide definitions to the Syra Health Disaster Recovery Plan [Abbreviated **D.R.**].

Disaster Recovery Plan

The Syra Health Disaster Recovery operations plan is split into 4 steps:

1. Disaster is declared. Stakeholders are informed, depending on severity and type of incident, an alert will be put out so that staff and customers are aware of the issue.
2. Systems designed with automatic failovers (Hot-Spare) do not require intervention and will automatically be restored to working order. Systems that do require intervention will proceed to the next step.
3. I.T. Will begin reviewing the outage to see when they occurred so the systems can be reverted to the last working configuration, whether by restoring from cold backups, or by pushing the spare system into production.
4. I.T. will perform a board of review to determine what the issue was. Inform stakeholders of their findings, and work on designing a system that will help mitigate the same issue in the future.

D.R. Classifications

All Syra Health systems will be reviewed on a periodic basis and failovers tested as needed to verify Company integrity and policies, and in compliance with federal and/or state laws. The systems designed for use are built on a tiered approach,

Key & Mission Critical Services

These systems are kept in triplicate (Hot-Spare) across multiple hosting and cloud providers, and regions. This can include but is not limited to: Application Servers and Services, Data Storage Infrastructure, Security & Identity provider solutions.

Data Backups

Data Backups are maintained as part all branches of this overview to ensure business continuity.

Mission Critical Systems are setup to have data mirroring established with at least 3 copies, 2 of which must be stored on separate environments and regions. Mission Critical systems are also archived hourly with a two-week cycle (Cold Vault) in the event the environment/system suffers an unrecoverable error.

Priority Business systems are established with data mirroring, where the systems can share the same cloud infrastructure / provider, but have to be located in separate regions. (I.E. One system is setup with an instance in an East Coast Cloud, and the second instance is in a West Coast Cloud)

Day to day computer operations are setup to have data mirroring in a minimum of 2 locations.

APPROVALS

<u><i>Zach Knibbs</i></u>	<u>Zach Knibbs</u>	<u>Director of Technology</u>	<u>2/6/23</u>
Signature	Name	Title	Date