Inodaya Hospitals	**INODAYA Hospitals - Kakinada**		**Documentation code: INH/IMS.Doc.03**
	IMS 1e.POLICY ON IT CONTINGENCY PLAN		**Prepared date:** 11/11/2025
	Reference: IMS.1e NABH Standards – 6th Edition		Issue Date: 11/11/2025
	Issue no: 01	Review No: 0	**Review date:** 10/11/2026

IMS 1e.POLICY ON IT CONTINGENCY PLAN

1. Purpose

To establish guidelines for maintaining or rapidly resuming critical IT services during a disruption, including cyber security incidents, data loss, natural disasters, or system outages, to ensure continuous operation of hospital services and patient safety.

2. Scope

Applies to all IT systems, networks, data, and services managed or supported by the IT Department, including EHR (Electronic Health Record) systems, hospital management systems, and communication infrastructure.

3. Policy Statement

The IT department shall maintain an IT contingency plan that includes strategies for:

- **System backups**
- **Disaster recovery**
- **Emergency operations**
- **Alternate data processing**
- **System restoration**

The policy ensures all mission-critical systems can be restored in a timely manner to minimize disruption to healthcare delivery.

Prepared by: D. Leela Veerababu	**Verified by:**	**Approved by:** G. Lakshmi Lavanya
Mr.Leela Veerababu.D	Dr.Gowtam krishna	Ms.Lakshmi Lavanya
Incharge – IT Dept	Medical director	Chief executive officer

4. Roles & Responsibilities

Role	Responsibility
IT Manager	Oversees development and implementation of the contingency plan
System Administrators	Ensure backup procedures are followed; support restoration
Helpdesk Team	Serve as the first point of contact in an incident
Compliance Officer	Ensures adherence to healthcare IT regulations (e.g., HIPAA)
Department Heads	Coordinate department-specific IT needs and report impacts

5. Procedures

5.1 Risk Assessment

Conduct annual risk assessments to identify critical systems and vulnerabilities.

5.2.1 Backup Strategy Overview

The hospital's IT department shall implement a **multi-tiered backup approach** consisting of:

1. **Daily backups** (incremental or differential)
2. **Weekly full backups** stored offsite or in a securing hard disk device

3. **Monthly validation and testing** to ensure backup integrity and recoverability

4. To protect important hospital data, the IT department will follow a clear and secure backup plan. This plan includes taking daily backups of critical systems like Electronic Health Records (EHR), Laboratory and Pharmacy systems, and key administrative

applications. These backups will be done automatically every day and saved securely on hospital servers. In addition, a full backup of all systems will be taken every week and stored at an offsite location (…………………………) or on a secure cloud service like **……………………….** using encrypted connections to keep the data safe.

5. The backup will cover all essential hospital data, including patient records, billing and finance information, emails, and system settings. All backups will be encrypted both when stored and during transfer, to ensure patient and hospital data remains protected. The hospital will keep daily backups for at least 30 days, weekly backups for 90 days, and monthly backups for one year or more, based on regulatory needs.

6. Only authorized IT staff will have access to backup systems, using secure logins and multi-factor authentication. Each month, the IT team will test selected backups by restoring them, to make sure the data can be recovered properly. Any backup problems will be fixed immediately and reported to IT management. Backup systems will be checked regularly, and alerts will notify the team of any issues like failed backups or low storage.

7. This backup process is critical for making sure the hospital continues to run smoothly, even if something goes wrong. It also ensures the hospital follows important healthcare rules such as HIPAA, NABH, and ISO/IEC 27001. The backup policy will be reviewed every year or whenever there are major changes in systems or technology.

8. Data Backup MOU with **Blue fox Technologies**

Prepared by: D. Leela Veerababu	**Verified by:**	**Approved by:** G. Lakshmi Lavanya
Mr.Leela Veerababu.D	Dr.Gowtam krishna	Ms.Lakshmi Lavanya
Incharge – IT Dept	Medical director	Chief executive officer