**U10A1 – Security Emergency Plan**

**Chris Misch**

School of Business, Technology, and Health Care Administration, Capella University

IT4076: Security Management and Policies

Stuart McCubbrey

June 2023

1. **Overview**

This policy lays out how to create and conduct emergency procedures in the event of natural or man-made disruptions to the day-to-day function of High Class Healthcare. The policy will include the IT, technical, and data contingency plan along with the outline of a contingency plan template.

* 1. **Purpose**

The purpose of this policy is to ensure that plans have been created to limit the impact of a major disruption to business. This policy will outline what polices need to be created and how they will affect the recovery of the organization back to acceptable buisness activity.

* 1. **Scope**

The scope of this policy will include all systems, networks, employees, contractors, vendors, and any other associates that conduct buisness with High Class Healthcare.

1. **Policy**

Policies developed and maintained will be integrated with the System Development Life Cycle (SDLC). This policy will follow the SDLC of risk, scenario, and trigger analysis along with plan development and return to full operations. This is to ensure the interoperability and integrity of all policies, systems, and controls while keeping to High Class Healthcare’s mission statement.

* 1. **IT Contingency Plan**

The IT Contingency Plan protects the organization’s systems and network from disruptions due to natural or man-mad disasters. The IT Contingency Plan consists of five components that ensure a comprehensive plan has been developed.

* + 1. **Supporting Information**
       1. The supporting information component will outline the essential background and contextual information making it easier to understand, implement, and maintain.
       2. The reasons for the implementation must be clear and easy to understand.
       3. Acceptable levels of risk will be measured through recovery time objectives (RTO), and recovery point objectives (RPO).
       4. Identify alternate recovery: hot, warm, or cold.
       5. Provide details of all information systems and platforms
       6. Provide a quick implementation overview of the activation and notification phase, recovery phase and reconstitution phase.
    2. **Activation and Notification Phase**
       1. Identify the main contacts who will be responsible for each type of emergency and who their alternate backup will be.
       2. Create a call phone tree that includes both main and alternate contacts names, positions, and at least 2 ways to contact them.
       3. Ensure that all Points of Contact (POC) can receive notification of current and ongoing notification.
       4. Emergency criteria and procedures will be developed that document the extent of damage, criticality of the damage, and RTO.
       5. An Outage assessment will be created documenting the nature and extent of the disruption.
    3. **Recovery Phase**
       1. Create a recovery time strategy that will restore all system capabilities, repair damage to effected areas, and resume normal operation.
       2. Assess what areas of the recovery must be done sooner, that were identified in the BIA.
       3. All procedures should be written clearly with step-by-step instructions.
       4. Identify escalation and notification procedures for different types of triggers or events.
       5. Develop procedures appropriate for each recovery team to follow. This can include obtaining authorized access, notifying business partners, obtaining replacement devices or equipment, backup data, reconnecting systems, testing systems, and ensuring equipment operates properly.
       6. Document all recovery and escalation situations.
    4. **Reconstitution Phase**
       1. Define what actions will be taken to test and validate system capability and functionality.
       2. Create measures that test to ensure normal operations are up and running.
       3. Document the successful validation and deactivation of the recovery plan.
       4. Ensure the emergency plan has been deactivated and ready for another disruption.
       5. Notify the ISCP of the return to normal operations.
       6. Perform a full data back up the restored systems immediately.
       7. Create a log that makes note of the successful recovery and return to expectable buisness activity.
    5. **Appendices**
       1. Any details not included in the body of the emergency plan will be included here along with vendor contact information, BIA, recovery procedures and check lists, validation testing, Vendor SLAs, and emergency contact information.

* 1. **Technical Contingency Plan**

The technical contingency plan is specific to the areas within IT platforms. Each plan will seek to reestablish normal working conditions to post-disruption. When creating each plan technical requirements must be considered along with technology-based solutions for each type of system.

* + 1. All technical contingency plans developed must include the following five common foundational steps:
       - 1. Use of information from BIA process to include resiliency and contingency planning and system RTO. The BIA will also help with assessing the proper need for data protection.
         2. Development of data security and integrity and backup policies and procedures that follow the data contingency plan.
         3. Adherence and compliance with NIST SP800-53
         4. Development of alternative and primary sites with robust power management and environmental controls set up.
         5. Use of High Availability (HA) processes ensuring real time access to alternate system resources. HA must achieve an uptime of 99.999% or better.
    2. Each platform used in High Class Healthcare will be identified and a contingency plan will be developed using the contingency plan template.
       1. Platforms will include but are not limited to cloud systems, client/server systems, telecommunication systems, mainframe/server systems, IoT systems, web and email systems, and protected health information data.
    3. The development of this plan will follow the SDLC to ensure proper actions have been taken to restore normal operations.
    4. Ensure each contingency pan is resilient to both environmental and component level failures.
  1. **Data Contingency Plan**

Data must be protected, and a contingency plan must be put into place to ensure confidentiality, integrity, and availability (C-I-A) is restored due to disruption of business. To do this a risk assessment must be conducted following the FIPS 199 assessment and guidelines in High Class Healthcare’s BIA. To ensure this is done correctly There are 3 categories that must be addressed.

* + 1. **Data Back up and restoration**.
       1. Backups must be conducted at regular intervals that do not exceed the RPO defined in the BIA.
       2. Backups must be stored at an offsite location that is secure with proper environmental controls installed. Offsite locations can be a physical location or cloud managed storage.
       3. The organization will make use of all three common backup methods: full, incremental, and differential.
       4. Backup sites must make use of HA processes to maximize system uptime.
       5. When storing data in backup systems use only the latest encryption standards as per HIPAA §164.306 regulations and ensure that measures are taken to ensure data integrity are used.
       6. Backups should not disrupt normal business routine.
    2. **Testing and review**
       1. Regular testing will be conducted a minimum of once a year. This will ensure data integrity is maintained and assured.
       2. Reviews of the data contingency plan will be conducted twice a year.
    3. **Maintenance and updates**
       1. System maintenance will be conducted quarterly to ensure backup devices are not corrupt.
       2. Updates to data storage and software will be assessed according to measured testing provided by High Class Healthcare BIA.

1. **Contingency Plan Template**

The contingency plan template will include an introduction, system description, and include the three main phases (Activation and Notification, Recovery, and Reconstitution) of the recovery plan specific to the system it is addressing. There will be 3 templates made: low-impact systems, medium-impact systems, and high-impact systems. The structure will follow the design in Appendix A of NIST SP800-34r.1 framework.

1. **Policy Compliance**

All individuals within High Class Healthcare and thoes selected to be on the emergency team must comply with this Policy. Failure to follow this policy will result in disciplinary action, up to and including termination of employment, services, or contracts. The IT security manager must be notified immediately of any violation of this policy or to your assigned department manager for further investigation or escalation.

1. **Roles and Responsibilities**

ISCP Coordinator – Communicates changes to the policy plans as necessary to respective representatives. Evaluate and ensure policy information is current and meets system requirements.

POC – ensure the impact caused by changes within the hospital will be reflected in the contingency plan.

CIO – Will activate the Contingency Plan in the case the CIO is not available the CEO will assume this responsibility.

CEO – Assumes final approval of this policy and is the successor to the CIO in activating the Contingency Plan.

1. **Related Standards, Policies and Procedures**

HIPAA §164.312 Technical safeguards

NIST SP800-34r.2

NIST SP800-53

FIPS 199

FISMA

BIA

1. **Definitions and Terms**

FIPS – Federal Information Processing Standards

FISMA – Federal Information Security Management Act

POC – Points of Contact

RPO -Recovery Point Objective. The acceptable amount of time allowed for the systems to be offline.

RTO – Return Time Objective. The time it takes to get all systems back online.

SDLC – System Development Life Cycle. Includes 5 phases: creating, developing, testing, maintaining, and disposing.

HA – High Availability

1. **Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Summary of Changes | Approval |
| 1.0 | 06/10/2023 | Creation of new policy | Mark Moneybags, CEO |

1. **Resources**

Beebe, S. (2022). 5 Steps Your Contingency Planning Should Include. *Synario*. <https://www.synario.com/5-step-contingency-planning/>